

Министерство образования и науки Российской Федерации
ФГБОУ ВО «Уральский государственный педагогический университет»
Институт математики, информатики и информационных технологий
Кафедра высшей математики

**Использование прикладного пакета GAP для описания решеток
подалгебр трехмерных алгебр над полем GF(2)**

Выпускная квалификационная работа

Квалификационная работа
допущена к защите
Зав. кафедрой

дата

подпись

Исполнитель:
Воронков Леонид Юрьевич,
обучающийся БП-51Z груп-
пы

подпись

Руководитель ОПОП:

подпись

Научный руководитель:
Коробков С.С.,
к.ф.-м.н., доцент

подпись

Екатеринбург 2016

Оглавление

Введение	3
ГЛАВА I. Теоретические основы	6
1.1. Основные алгебраические структуры	6
1.2. Понятие алгебры над полем, примеры алгебр	11
1.3. Алгебра матриц над полем	12
1.4. Понятие подалгебры, признак подалгебры	13
1.5. Понятие решетки, основные свойства решеток	13
1.6. Диаграммы решеток	15
1.7. Алгебраические элементы колец	16
1.8. Пирсовские разложения колец	17
ГЛАВА II. Система компьютерной алгебры GAP	19
2.1. Общая характеристика пакета GAP	19
2.2. Язык программирования GAP	21
Общие команды пакета.	22
2.3. Команды для вычислений в алгебрах	25
ГЛАВА III. Типовая классификация трехмерных подалгебр алгебры матриц $M(GF(2),3)$	29
3.1. Трехмерные подалгебры алгебры матриц над полем из двух элементов	29
3.2. Вычисление типов решеток подалгебр	43
3.3. Выяснение отношения покрытия на множестве подалгебр	44
3.4. Построение диаграмм	54
Литература	58
Приложение	59

Введение

В выпускной квалификационной работе была рассмотрена алгебра $A = M_3(GF(2))$ квадратных матриц 3 порядка над полем $F = GF(2)$ из двух элементов. Главным объектом исследования являются трехмерные подалгебры алгебры A и их решётки подалгебр.

В работе используется понятие типа решетки подалгебр, введём это понятие.

Определение 1. Пусть S – подалгебра алгебры $M_3(GF(2))$ содержащая 2^n элементов. Назовем упорядоченную последовательность (m_0, m_1, \dots, m_n) *типом* решётки подалгебр алгебры S , если m_i – число подалгебр в S порядка 2^i , где $i = 0, 1, \dots, n$.

Целью исследования является разработка алгоритмов и программ для получения классификации трехмерных подалгебр алгебры $M_3(GF(2))$, описания типов решёток подалгебр и построения диаграмм решёток. Описание подалгебр должно быть приведено на языке порождающих элементов и определяющих их соотношений.

Для достижения основной цели решаются следующие **задачи**:

1. Разработка алгоритмов и программ для построения трехмерных подалгебр на языке образующих элементов.
2. Разработка алгоритмов и программ для определения типов решёток подалгебр и построение диаграмм.
3. Классифицировать подалгебры по типам решёток подалгебр.

Все задачи решаются с помощью системы компьютерной алгебры **GAP**.

Работа состоит из введения, трех глав, списка литературы и приложений.

В первой главе приводятся необходимые теоретические понятия. В ней содержится определение алгебры над полем, приводятся примеры алгебр, понятие подалгебры и формулируется признак подалгебры. Там же указано определение решётки и указываются основные свойства решёток.

Все вычисления проходят в системе компьютерной алгебры **GAP**, поэтому необходимые сведения о системе компьютерной алгебры **GAP** и её основных командах приводятся во второй главе.

В третьей главе содержится практическая часть. Здесь приводятся описания всех немоногенных трехмерных подалгебр алгебры $M_3(GF(2))$, даётся их полная классификация как на языке определяющих соотношений, так и типовая классификация.

Основные результаты, полученные в работе, приведены в таблице № 1.

Таблица №1

№	Порождающие элементы	Определяющие соотношения	Количество подалгебр	Тип решетки подалгебр
1	e_1, e_2, r	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j$, $e_1 r = r e_1 = 0, e_2 r = r e_2 = r$	84	(1,4,4,1) Рисунок 1
2	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, e r_1 = r_1 e = r_1,$ $e r_2 = r_2 = r_2 e$	14	(1,4,4,1) Рисунок 2
3	r_1, r_2	$r_1^3 = 0, r_1^2 \neq 0, r_2^2 = 0, r_1 r_2 = r_1^2,$ $r_2 r_1 = 0$	21	(1,5,3,1) Рисунок 3
4	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, e r_1 = r_1 e = 0,$ $e r_2 = r_2, r_2 e = 0$	42	(1,5,4,1) Рисунок 4
5	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, e r_1 = r_1 e = 0,$ $e r_2 = 0, r_2 e = r_2$	42	(1,5,4,1) Рисунок 4
6	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, e r_1 = r_1 e = r_1,$ $e r_2 = r_2, r_2 e = 0$	42	(1,5,4,1) Рисунок 4

7	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, er_1 = r_1 e = r_1,$ $er_2 = 0, r_2 e = r_2$	42	(1,5,4,1) Рисунок 4
8	e_1, e_2, r	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j,$ $e_1 r = r e_1 = 0, e_2 r = 0, r e_2 = r$	84	(1,6,5,1) Рисунок 5
9	e_1, e_2, r	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j,$ $e_1 r = r e_1 = 0, e_2 r = r, r e_2 = 0$	84	(1,6,5,1) Рисунок 5
10	e_1, e_2, r	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j,$ $e_2 r = r e_1 = 0, e_1 r = r = r e_2$	168	(1,6,5,1) Рисунок 5
11	e_1, e_2, e_3	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j$	28	(1,7,6,1) Рисунок 6
12	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, er_i = 0,$ $r_i e = r_i$	14	(1,7,7,1) Рисунок 7
13	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, r_i e = 0,$ $er_i = r_i$	14	(1,7,7,1) Рисунок 7
		ИТОГО:	679	6

В результате расчётов, было выяснено, что внутри каждого типа, за исключением типа (1, 4, 4, 1), подалгебры имеют изоморфные решётки, а подалгебры с типом решётки (1, 4, 4, 1) разделяются на два подмножества и имеют неизоморфные решётки подалгебр.

ГЛАВА I. Теоретические основы

1.1. Основные алгебраические структуры

Определение 2. Группой называется множество G с алгебраической операцией \cdot , если выполняются следующие условия:

- 1) операция \cdot в G ассоциативна: $\forall a, b, c \in G (a \cdot (b \cdot c) = (a \cdot b) \cdot c)$;
- 2) в G существует нейтральный элемент 1 : $\forall a \in G (a \cdot 1 = 1 \cdot a = a)$;
- 3) для каждого элемента $a \in G$ существует обратный ему элемент $a^{-1} \in G$: $(a \cdot a^{-1} = a^{-1} \cdot a = 1)$.

Если операция \cdot коммутативна, то группа называется коммутативной, или абелевой. В противном случае группа называется некоммутативной.

Относительно операции сложения группами являются множества Z , Q , R . Относительно операции умножения группами являются множества $Q \setminus \{0\}$ и $R \setminus \{0\}$ отличных от нуля рациональных и действительных чисел. Все эти группы коммутативные.

В группах по сложению нейтральный элемент 0 называют нулевым (или просто нулем), а обратный элемент a^{-1} – противоположным ($-a$). В группах по умножению нейтральный элемент 1 называют единичным (или просто единицей).

Пример 1. Доказать, что множество $\{0\}$, состоящее из одного числа нуль, образует коммутативную группу по сложению.

Действительно, операция сложения определена на указанном множестве, так как $0 + 0 = 0$. Из этого равенства следует, что этот единственный элемент множества служит нулевым (нейтральным) элементом, а также противоположным (обратным) для себя. Ассоциативность сложения очевидна: $(0 + 0) + 0 = 0 + (0 + 0)$. Следовательно, все (три) условия в определении группы выполняются.

Учитывая коммутативность сложения, заключаем, что рассматриваемое множество – коммутативная группа.

Пример 2. Доказать, что множество $\{+1, -1\}$, состоящее из двух чисел, образует коммутативную группу по умножению.

Действительно, операция умножения определена на указанном множестве, так как

$$(+1) \cdot (+1) = +1, (+1) \cdot (-1) = (-1) \cdot (+1) = -1, (-1) \cdot (-1) = +1.$$

Следовательно, произведение элементов есть элемент того же множества. Ассоциативность умножения очевидна. Из равенств следует, что существует единичный элемент $e = +1$. Кроме того, каждый элемент имеет обратный: $(+1)^{-1} = +1, (-1)^{-1} = -1$. Таким образом, все (три) условия в определении группы выполняются. Из равенств следует, что умножение коммутативно, поэтому данная группа коммутативная.

Определение 2[15]. Множество K , на котором заданы две операции – сложение $(+)$ и умножение (\cdot) , называется кольцом, если выполняются следующие условия:

1) относительно операции сложения множество K – коммутативная группа, т.е.

– операция сложения коммутативна:

$$(\forall a \in K) (\forall b \in K) (a + b = b + a);$$

– операция сложения ассоциативна:

$$(\forall a \in K) (\forall b \in K) (\forall c \in K) (a + (b + c) = (a + b) + c);$$

– существует нулевой элемент 0 : $(\forall a \in K) (a + 0 = 0 + a = a)$;

– для каждого элемента $a \in K$ существует противоположный ему элемент $(-a) \in K$: $(a + (-a) = (-a) + a = 0)$;

2) операция умножения в множестве K ассоциативна:

$$\forall a \in K \forall b \in K \forall c \in K (a \cdot (b \cdot c) = (a \cdot b) \cdot c);$$

3) операции сложения и умножения связаны законами дистрибутивности:

$$(a + b) \cdot c = a \cdot c + b \cdot c \quad \text{и} \quad c \cdot (a + b) = c \cdot a + c \cdot b \quad \forall a \in K$$

$$, \quad \forall b \in K, \quad \forall c \in K.$$

Если операция умножения коммутативна: $a \cdot b = b \cdot a$, то кольцо называется коммутативным, в противном случае кольцо называется некоммутативным. Если для операции умножения существует единичный элемент e : $a \cdot e = e \cdot a = a$, то говорят, что кольцо K – есть кольцо с единицей.

Кольцами являются множества целых, рациональных, действительных чисел, причем все они – коммутативные кольца с единицей. Примеры других колец, в том числе и некоммутативных, встретятся в дальнейшем. Как видим, кольцо – это множество, в котором определены три операции: сложение, умножение и вычитание.

Рассмотрим подробнее законы дистрибутивности. Пусть на множестве K заданы две операции сложение $(+)$ и умножение (\cdot) . Операция \cdot называется дистрибутивной слева относительно операции $+$, если для любых a, b, c из K

$$c \cdot (a + b) = (c \cdot a) + (c \cdot b),$$

и дистрибутивной справа относительно операции $+$, если

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

Если операция \cdot коммутативна, то дистрибутивность слева операции \cdot относительно операции $+$ влечет дистрибутивность справа, так как

$$(a + b) \cdot c = c \cdot (a + b) = (c \cdot a) + (c \cdot b) = (a \cdot c) + (b \cdot c).$$

В этом случае говорят, что операция \cdot дистрибутивна относительно операции $+$. Например, операция умножения чисел дистрибутивна (слева и справа) относительно операции сложения чисел. Следующий пример показывает, что имеются операции с "односторонней" дистрибутивностью.

Пример 3 Рассмотрим множество R^+ положительных действительных чисел. На этом множестве определим две операции: умножения $(a \cdot b)$ и возведе-

ния в положительную степень ($a \uparrow b = a^b$). Доказать, что операция \uparrow возведения в степень дистрибутивна справа относительно умножения, но не дистрибутивна слева.

В самом деле, для любых положительных действительных чисел a, b, c справедливы равенства

$$(a \cdot b) \uparrow c = (a \cdot b)^c = a^c \cdot b^c = (a \uparrow c) \cdot (b \uparrow c).$$

Следовательно, операция \uparrow дистрибутивна справа относительно операции умножения чисел. Дистрибутивность \uparrow слева относительно умножения опровергается примером

$$2 \uparrow (3 \cdot 2) = 2^{3 \cdot 2} = 2^6 = 64 \neq 32 = 2^3 \cdot 2^2 = (2 \uparrow 3) \cdot (2 \uparrow 2).$$

Пример 4 Доказать, что множество чисел вида

$$m + n\sqrt{2},$$

где m и n – целые числа, является кольцом.

Действительно, операции сложения и умножения определены на рассматриваемом множестве, так как сумма и произведение двух чисел вида $m + n\sqrt{2}$ имеют тоже самое представление:

$$(m_1 + n_1\sqrt{2}) + (m_2 + n_2\sqrt{2}) = (m_1 + m_2) + (n_1 + n_2)\sqrt{2};$$

$$(m_1 + n_1\sqrt{2}) \cdot (m_2 + n_2\sqrt{2}) = (m_1m_2 + 2n_1n_2) + (m_1n_2 + m_2n_1)\sqrt{2}.$$

Числа $(m_1 + m_2), (n_1 + n_2), (m_1m_2 + 2n_1n_2), (m_1n_2 + m_2n_1)$, очевидно, целые для любых целых m_1, m_2, n_1, n_2 . Законы коммутативности, ассоциативности и дистрибутивности не нуждаются в проверке, так как речь идет о сложении и умножении действительных чисел. Нулевым элементом служит число $\theta = 0 + 0\sqrt{2}$. Для каждого числа $m + n\sqrt{2}$ противоположным элементом является число $(-m) + (-n)\sqrt{2}$, так как

$$(m + n\sqrt{2}) + ((-m) + (-n)\sqrt{2}) = (m - m) + (n - n)\sqrt{2} = 0 + 0\sqrt{2}.$$

Таким образом, рассматриваемое множество удовлетворяет всем условиям определения кольца.

Определение 3[15] Множество F , на котором заданы две операции: сложение $(+)$ и умножение (\cdot) , называется полем, если выполняются следующие условия:

- 1) F – коммутативное кольцо с единицей ($e \neq \theta$);
- 2) для каждого элемента $a \in F$, отличного от нулевого ($a \neq \theta$), существует обратный элемент $a^{-1} \in F$: $a \cdot a^{-1} = e$.

Как видим, поле – это множество, в котором определены четыре операции: сложение, умножение, вычитание и деление. Полями, например, являются множества рациональных и действительных чисел.

Замечание. Можно доказать, что числовое множество $M_p = \{0, 1, 2, \dots, p-1\}$ операциями "сложения по модулю p " и "умножения по модулю p " является полем для любого простого числа p .

Пример 5. Доказать, что множество чисел вида

$$p + q\sqrt{2},$$

где p и q – рациональные числа, является полем.

Действительно, операции сложения и умножения определены на рассматриваемом множестве, так как сумма и произведение двух чисел вида $p + q\sqrt{2}$ имеют тоже самое представление:

$$(p_1 + q_1\sqrt{2}) + (p_2 + q_2\sqrt{2}) = (p_1 + p_2) + (q_1 + q_2)\sqrt{2};$$

$$(p_1 + q_1\sqrt{2}) \cdot (p_2 + q_2\sqrt{2}) = (p_1p_2 + 2q_1q_2) + (p_1q_2 + p_2q_1)\sqrt{2}.$$

Числа $(p_1 + p_2)$, $(q_1 + q_2)$, $(p_1p_2 + 2q_1q_2)$, $(p_1q_2 + p_2q_1)$, очевидно, рациональные для любых рациональных p_1, p_2, q_1, q_2 . Законы коммутативности, ассоциативности и дистрибутивности не нуждаются в проверке, так как речь идет о сложении и умножении действительных чисел. Нулевым элементом служит число $\theta = 0 + 0\sqrt{2}$. Для каждого числа $p + q\sqrt{2}$ противоположным элементом является число $(-p) + (-q)\sqrt{2}$, так как

$$(p + q\sqrt{2}) + ((-p) + (-q)\sqrt{2}) = (p - p) + (q - q)\sqrt{2} = 0 + 0\sqrt{2}.$$

Таким образом, рассматриваемое множество является коммутативным кольцом с единицей ($e \neq \theta$). Осталось показать, что любое число $p + q\sqrt{2}$, отличное от нулевого элемента $\theta = 0 + 0\sqrt{2}$, имеет обратный. В самом деле, учитывая, что

$$\frac{1}{p + q\sqrt{2}} = \frac{p - q\sqrt{2}}{(p + q\sqrt{2})(p - q\sqrt{2})} = \frac{p}{p^2 - 2q^2} - \frac{q}{p^2 - 2q^2}\sqrt{2},$$

определим обратный элемент равенством

$$(p + q\sqrt{2})^{-1} = \frac{p}{p^2 - 2q^2} - \frac{q}{p^2 - 2q^2}\sqrt{2}.$$

Тогда

$$\begin{aligned} (p + q\sqrt{2}) \cdot (p + q\sqrt{2})^{-1} &= (p + q\sqrt{2})^{-1} \cdot (p + q\sqrt{2}) = \\ &= (p + q\sqrt{2}) \cdot \left(\frac{p}{p^2 - 2q^2} - \frac{q}{p^2 - 2q^2}\sqrt{2} \right) = 1 + 0\sqrt{2} = e. \end{aligned}$$

Заметим, что знаменатель $p^2 - 2q^2$ отличен от нуля для любых рациональных чисел p и q , не равных нулю одновременно. Действительно, равенство $p^2 = 2q^2$ равносильно равенству $|p| = |q| \cdot \sqrt{2}$, а это означает, что $\sqrt{2}$ – рациональное число. Поскольку число $\sqrt{2}$ – иррациональное, значит $p^2 - 2q^2 \neq 0$, т.е. обратный элемент существует для любого $p + q\sqrt{2} \neq 0$.

Так как рассматриваемое множество является коммутативным кольцом с единицей и каждый элемент, отличный от нуля, имеет обратный, то оно является полем.

1.2. Понятие алгебры над полем, примеры алгебр

Определение 2[8]. Алгеброй над полем F называется множество A , на котором определены две бинарные операции $+$ и \cdot , а также операция умножения элементов из F на элементы из A (то есть отображение $F \times A \rightarrow A$), удовлетворяющее следующим условиям:

- 1) $(A, +, \cdot)$ – кольцо;
- 2) $(A, +)$ – векторное пространство над полем F ;

$$3) \forall \alpha \in F \forall a, b \in A ((\alpha a)b = \alpha(ab) = a(\alpha b)).$$

Пример 1.

Пусть $M_n(F) = \{(\alpha_{ij}) \mid \alpha_{ij} \in F\}$ – множество всех квадратных матриц с коэффициентами из поля F . Понятно, что $M_n(F)$ – кольцо относительно операций сложения и умножения квадратных матриц. Если определим умножение элементов из F на элементы из $M_n(F)$ таким образом:

$$\forall \beta \forall (\alpha_{ij}) \in M_n(F) \beta(\alpha_{ij}) = (\beta \alpha_{ij}),$$

то относительно такого умножения и сложения матриц множество $M_n(F)$ становится векторным пространством над полем F .

Пусть $a = (\alpha_{ij})$, $b = (\beta_{ij})$, $\alpha \in F$. Тогда $(\alpha a)b = (\alpha \alpha_{ij})(\beta_{ij}) = (\sum \alpha \alpha_{ij} \beta_{ij}) = (\sum \alpha_{ij}(\alpha \beta_{ij})) = a(\alpha b) = (\alpha(\sum \alpha_{ij} \beta_{ij})) = \alpha(ab)$.

Отсюда следует, $M_n(F)$ – алгебра над полем F . Эта алгебра называется *алгеброй матриц над полем F* .

Пример 2.

Пусть K – расширение поля P . Тогда

- 1) K – кольцо;
- 2) $(K, +)$ – векторное пространство над полем P ;
- 3) $\forall \alpha \in P \forall a \in K \alpha a$ – произведение элементов в поле K и $\alpha(ab) = (\alpha a)b = a(\alpha b)$. Следовательно, K – алгебра над полем P .

1.3. Алгебра матриц над полем

Определение 3[8]. Пусть A — алгебра над полем P . Назовем алгебру A *конечномерной*, если A , как векторное пространство над полем P , *конечномерно*. При этом размерность векторного пространства A над P будем называть *размерностью* или *рангом* алгебры A .

Пример 3.

Пусть $A = C$, $P = R$. Тогда числа $1, i$ образуют базис C над R и потому $\dim C = 2$.

Пример 4.

Базис алгебры $M_n(F)$ образуют матричные единицы $E_{ij} = (e_{ij})$, где $e_{ij} = 0$, если $i \neq j$ и $e_{ij} = 1$, если $i = j$. Следовательно, $\dim M_n(F) = n^2$.

1.4. Понятие подалгебры, признак подалгебры

Определение 4 [8]. Подмножество S алгебры A над полем P назовем *подалгеброй алгебры A* , если относительно операций, определенных в A , S само является алгеброй над полем P .

Признак подалгебры: Непустое подмножество S алгебры A над полем P тогда и только тогда является подалгеброй в A , когда выполнены следующие условия:

- 1) $\forall a, b \in S \quad a - b \in S$;
- 2) $\forall a, b \in S \quad a \cdot b \in S$;
- 3) $\forall \alpha \in P \quad \forall a \in S \quad \alpha a \in S$.

Доказательство. Пусть S – подалгебра алгебры A . Тогда очевидно, что условия 1)–3) выполнены. Обратно: пусть выполнены условия 1)–3). Тогда из выполнимости условий 1) и 2) следует, что S – подкольцо кольца A , а из выполнимости условий 1) и 3) следует, что S – векторное подпространство пространства A . Условие 3) определения 3.1. выполняется в S , так как оно выполняется в A . Таким образом, S – подалгебра алгебры A .

1.5. Понятие решетки, основные свойства решеток

Определение 5 [6]. Верхней границей подмножества S частично упорядоченного множества (ч.у. множества) (P, \leq) называется элемент $a \in P$, удовлетворяющий условию $(\forall s \in S \quad s \leq a)$.

Определение 6 [6]. Верхней гранью (или супремумом) подмножества S ч.у. множества (P, \leq) называется наименьший элемент в множестве верхних границ подмножества S .

Из определения 5 следует, что верхняя грань подмножества определяется однозначно (в отличие от верхней границы). Верхнюю грань подмножества S в подмножестве $T \subseteq P$ обозначают выражением $\sup_T S$, при этом индекс T , как правило, опускают, если $T = P$.

Определение 7 [6]. Двойственными понятиями верхней границы и верхней грани являются понятия *нижней границы* и *нижней грани*. Нижнюю грань называют также *инфимумом*. Нижнюю грань подмножества S в подмножестве $T \subseteq P$ обозначают символом $\inf_T S$ или символом $\inf S$ в случае, когда $T = P$. Двойственным образом устанавливается, что $\inf \emptyset$ существует тогда и только тогда, когда P содержит наименьший элемент 1 и что $\inf \emptyset = 1$.

Определение 8 [6]. Решеткой (или структурой) называется ч. у. множество, в котором каждое двухэлементное подмножество имеет нижнюю и верхнюю грани.

Определение 9 [6]. Полной решеткой называется ч. у. множество, в котором каждое подмножество имеет нижнюю и верхнюю грани.

Из этих определений следует, что любая полная решетка является решеткой. Но не наоборот.

Определение 10 [6]. Решеткой (или структурой) называется непустое множество L с определенными на нем двумя бинарными операциями \vee и \wedge , удовлетворяющие следующим условиям:

1. $\forall a \in L \ a \wedge a = a, \ a \vee a = a$ (идемпотентность);
2. $\forall a, b \in L \ a \wedge b = b \wedge a, \ a \vee b = b \vee a$ (коммутативность);
3. $\forall a, b, c \in L \ a \vee (b \wedge c) = (a \vee b) \wedge c, \ a \wedge (b \vee c) = (a \wedge b) \vee c$ (ассоциативность);
4. $\forall a, b \in L \ a \vee (a \wedge b) = a \wedge (a \vee b) = a$ (поглощения).

Свойства решеток.

Лемма 1 [6]. Во всякой решетке (L, \wedge, \vee) операции объединения и пересечения удовлетворяют условию изотопности: если $a \leq b$, то $a \wedge c \leq c \wedge b$ и $a \vee c \leq c \vee b$.

Лемма 2 [6]. Во всякой решетке (L, \wedge, \vee) выполняются следующие неравенства дистрибутивности:

$$(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c);$$

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c).$$

Лемма 3. Во всякой решетке (L, \wedge, \vee) выполняется неравенство модулярности: если $a \leq c$, то $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

1.6. Диаграммы решеток

Назовем элементы a и b ч.у. множества (P, \leq) *сравнимыми*, если $a \leq b$ или $b \leq a$. Будем считать, что элемент b покрывает элемент a , если выполнены следующие условия: 1) $a < b$; 2) $\forall c \in P ((a \leq c) \wedge (c \leq b) \rightarrow (c = a) \vee (c = b))$. Если b покрывает a , то будем записывать это кратко в таком виде: $a < b$.

В некоторых случаях ч.у. множество может быть изображено в виде диаграммы на плоскости. Для того чтобы изобразить ч.у. множество (P, \leq) в виде диаграммы, примем следующие соглашения:

1. Различные элементы множества P изображаются различными точками плоскости;
2. если $a, b \in P$ и b покрывает a , то точки, изображающие эти элементы, соединяются отрезком, причем точка, соответствующая b , располагается выше точки, соответствующей a .

Мы понимаем, что диаграмму можно построить полностью лишь в том случае, когда ч.у. множество P конечно. Однако при этом оно может быть достаточно сложной и потому совершенно бесполезной. Очевидно также и то, что при построении диаграммы ее отрезки могут пересекаться в точках, не изображающих элементов множества P . Диаграмма, содержащая минимальное число таких пересечений, называется *оптимальной*, а не содержащая их совсем – *плоской*.

Пример 5. $P = (M, \leq)$, где $M = \{1, 2, 5, 7\}$ (рис.1);

Пример 6. $S = (M, |)$, где $M = \{2, 3, 4, 6, 12\}$ (рис.2).



Рис.1

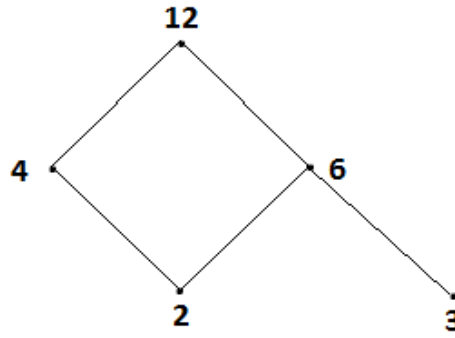


Рис.2

1.7. Алгебраические элементы колец

Любая алгебра является кольцом с операциями сложения (+) и умножения (*). $A = (A, +, *, \times)$, P – поле, $P = GF(2) = \{0, 1\}$.

Определение 10[9]. Элемент e кольца K называется идемпотентным элементом, если $e^2 = e$.

Пример7. Единица – в кольце Z .

$$m = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, m^2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Определение 11[9]. Элемент r кольца K называется нильпотентным, если $\exists n \in \mathbb{N}: r^n = 0$. Наименьший n с таким свойством называется индексом нильпотентности элемента n ($indr = n$).

Пример8. $0^2 = 0, ind\ 0 = 1$.

$$r = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, r^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0,$$

$$indr = 2.$$

$$m = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, m^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, m^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$ind\ m = 3.$$

Определение 12[9]. Элемент a кольца K называется алгебраическим, если существует многочлен положительной степени $f(x)$ с целыми коэффициентами, то есть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x$ такой, что $f(a) = 0$.

1.8. Пирсовские разложения колец

Пусть K – коммутативное кольцо, e – ненулевой идемпотентный элемент.

Определим два следующих множества:

- 1) $eK = \{ex | x \in K\} \neq \emptyset$;
- 2) $(1 - e)K = \{x - ex | x \in K\} \neq \emptyset$.

Докажем, что eK и $(1 - e)K$ – подкольца в K .

Признаком подкольца считается:

1. $\forall a, b \in S ((a - b) \in S)$
2. $\forall a, b \in S (ab \in S)$

Пусть $S = eK, a = ex_1, b = ex_2$.

- 1) $a - b = e(x_1 - x_2) \in eK$
- 2) $ab = ex_1 ex_2 = e^2 x_1 x_2 = e(ex_1 x_2) \in eK$

Пусть $S = (1 - e)K, a = (1 - e)x_1, b = (1 - e)x_2$.

- 1) $a - b = x_1 - x_2 - e(x_1 - x_2) = (1 - e)(x_1 - x_2) \in (1 - e)K$
- 2) $ab = (1 - e)x_1(1 - e)x_2 = (1 - e)((1 - e)x_1 x_2) \in (1 - e)K$

$eK + (1 - e)K = K$ – докажем это:

Пусть $x \in K$. Тогда $x = ex + (1 - e)x = ex + x - ex = x$.

Значит $K \subseteq eK + (1 - e)K$. Так как $eK, (1 - e)K \subseteq K$, то $eK + (1 - e)K = \{ex + (1 - e)y = ex + y - ey | x, y \in K\} \subseteq K$.

Убедимся в том, что $eK \cap (1 - e)K = \{0\}$.

Пусть $a \in eK \cap (1 - e)K$. Тогда $\exists x, y \in K$ такие, что

$$a = ex = (1 - e)y$$

$$ea = e(ex) = e(1 - e)y = e(y - ey) = ey - ey = 0 \Rightarrow a = 0$$

Обозначим $eK + (1 - e)K = eK \oplus (1 - e)K$ – прямая сумма двух подколец.

Таким образом: $K = eK \oplus (1 - e)K$ – пирсовское разложение кольца K по идемпотенту e . Видим, что $\forall a \in eK \quad ea, \text{ то есть } e - \text{единичный элемент в под-}$
 кольце eK . Аналогично этому $\forall c \in (1 - e)K \quad ec = 0$. Отсюда следует, если $x \in eK$, а $y \in (1 - e)K$, то $e(x + y) = x \Rightarrow xy = 0$.

Пусть K – некоммутативное кольцо, e – идемпотентный элемент. Тогда, если e – не единица, то имеет место двустороннее пирсовское разложение:

$$\begin{aligned} K &= eKe \oplus eK(1 - e) \oplus (1 - e)Ke \oplus (1 - e)K(1 - e), \\ eKe &\in a, eK(1 - e) \in b, (1 - e)Ke \in c, (1 - e)K(1 - e)d, \\ ba &= 0, ab \in eK(1 - e), \\ ac &= 0, ca \in (1 - e)Ke, \\ ad &= da = 0, \\ b^2 &= 0, c^2 = 0. \end{aligned}$$

S – трехмерные. $S = \langle a_1, a_2, a_3 \rangle, a_1, a_2, a_3$ – базис. $\forall a \in S \exists \lambda_1, \lambda_2, \lambda_3 \in \{0, 1\} a = \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3$. $S = \langle e_1, e_2, r \rangle, e_i^2 = e_i, r^2 = 0$
 $e_1 r = r, r e_1 = 0, e_2 r = 0, r e_2 = r, e_1 e_2 = e_2 e_1 = 0$.

ГЛАВА II. Система компьютерной алгебры GAP

2.1. Общая характеристика пакета GAP

GAP[13] –система компьютерной алгебры, доступная в свободном пользовании, открытая и расширяемая, название которой означает "Groups, Algorithms and Programming". Название программы было выбрано исключительно описывающие основные действия программы. GAP является системой компьютерной алгебры, придуманной как инструмент вычислительной теории групп, и впоследствии распространившийся на смежные разделы алгебры. В настоящее время **GAP** является уникальным всемирным совместным научным проектом, объединяющим специалистов в области алгебры, теории чисел, математической логики, информатики и др. наук из различных стран всего мира. Разработка системы началась в 1986 г. Первоначально **GAP** разрабатывался в г.Аахен, Германия (Lehrstuhl D für Mathematik, RWTH). В настоящее время центр разработки GAP и технической поддержки его пользователей находится в Шотландии (School of Mathematical and Computational Sciences, University of St. Andrews). Первая версия программы была написана студентом по имени Martin Schönert. Программа была написана на языке C.

Основные особенности GAP:

- используется язык программирования, внешне напоминающий Паскаль;
- используются общепринятые, стандартные типы основных алгебраических объектов: групп (абстрактных, матричных, подстановок), колец, полей;
- в системе доступны удобные типы переменных, а так же оперативно изменяемые списки и записи;
- доступно более 4 тысяч библиотечных функций;
- доступная всем обширная библиотека данных, включая практически все группы, порядок которых не превосходит 1000;

- вместе с **GAP** поставляются прикладные программы, охватывающие такие разделы алгебры, как комбинаторная теория групп, конечные простые группы, теория представлений групп, теория графов, в т.ч. их группы автоморфизмов, теория кодирования, кристаллографические группы, группы Галуа и многое другое;
- подробное и удобное описание (около 1600 стр.) в формате «гипертекст»;
- бесплатное получение по сети Internet вместе с исходными текстами, являющимися незаменимым и необходимым наглядным пособием для освоения GAP;
- работа в операционных системах DOS, Windows, Unix, Linux, MacOS;
- работа с процессором типа 386 и выше с ОЗУ от 8 Mb;
- система занимает на жёстком диске - от 10 до 100 Mb в зависимости от объема инсталляции;
- способность работать с ОЗУ до 128Mb и файлом подкачки до 128 Mb.

GAP дает возможность производить вычисления с огромными целыми и рациональными числами, допустимые значения которых ограничены только объемом доступной памяти. Далее, система работает с конечными полями, многочленами от многих переменных, рациональными функциями, векторами и матрицами. Пользователю доступны различные комбинаторные функции, элементарные теоретико-числовые функции, разнообразные функции для работы с множествами и списками.

Группы могут быть заданы в различной форме, например, как группы подстановок, матричные группы, группы, заданные порождающими элементами и определяющими соотношениями. Более того, построив, например, групповую алгебру, можно вычислить ее мультипликативную группу, и даже задать ее подгруппу, порожденную конкретными обратимыми элементами групповой

алгебры. Ряд групп может быть задан непосредственным обращением к библиотечным функциям (например, симметрическая и знакопеременная группы, группа диэдра, циклическая группа и др.).

Функции для работы с группами включают определение порядка группы, вычисление классов сопряженных элементов, центра и коммутанта группы, верхнего и нижнего центрального рядов, ряда коммутантов, Силовских подгрупп, максимальных подгрупп, нормальных подгрупп, решеток подгрупп, групп автоморфизмов, и т.д.

Теория представлений групп также входит в область применения системы GAP. Здесь имеются инструменты для вычисления таблиц характеров конкретных групп, действий над характерами и интерактивного построения таблиц характеров, определения теоретико-групповых свойств на основании свойств таблицы характеров группы. Модулярные представления групп (т.е. представления над полем, характеристика которого делит порядок группы) также могут быть исследованы с помощью GAP.

В версии 4.3 были существенным образом расширены возможности для работы с векторными пространствами, алгебрами и модулями. В системе могут быть определены векторные пространства над всеми доступными полями и модули над всеми доступными кольцами. Имеются алгоритмы для вычисления структуры конечномерных алгебр Ли, которые могут быть, например, заданы структурными константами или порождающими элементами, вычисления различных их Лиевских подалгебр и идеалов.

2.2. Язык программирования GAP

Ключевые слова.

Ключевыми словами GAP являются следующие слова: and, do, elif, else, end, fi, for, function, if, in, local, mod, not, od, or, repeat, return, then, until, while, quit, QUIT, break, rec, continue.

Общие команды пакета.

Приведем список специфических команд системы GAP, используемых в программах данной работы:

Список специфических команд системы GAP

MatAlgebra(GF(n),m)	# Построение алгебры матриц порядка m над полем, состоящим из n элементов
Elements(A)	# Элементы множества A
Dimension(A)	# Размерность алгебры A
Subalgebra(A,[m])	# Создание подалгебры алгебры A , порожденной элементом m
<u>Работа со списками и множествами:</u> N:=[]	# Создание пустого множества N
Size(N)	# Количество элементов множества N
AddSet(N,m)	# Присоединение элемента m к множеству N
Position(N,m)	# Порядок элемента m в списке N
IsSubsetSet(N,M)	# Проверяет, содержится ли каждый элемент множества M во множестве N
IntersectSet(N,M)	# Пересекает множество N с множеством M
UniteSet(N,M)	# Объединение множества N с множеством M
SubtractSet(N,M)	# Вычитает множество M от множества N , т.е. удаляет из множества M все элементы множества N
<u>Условный оператор:</u> if Q1 then P1; fi;	# Если $Q1$ - истина, то выполняется команда $P1$
if Q1 then P1; elif Q2 then A2; fi;	# Если $Q1$ - истина, то выполняется команда $P1$, а если $Q2$ - истина, то выполняется команда $P2$
<u>Работа с циклами:</u> for a in N do P; od;	# Для всех элементов множества N выполняется команда P
for i in [1..m] do P; od;	# Выполнение команды P m раз
<u>Работа с данными:</u> PrintTo(“***.dan”, N)	# Записывает данные в файл
Read(“***.dan”)	# Читает файл
quit;	# Выход из программы

Выражения.

Примерами выражений являются: переменные, обращения к функциям, целые числа, перестановки, строки, функции, списки, записи. С помощью опе-

раторов из них могут быть составлены более сложные выражения. Операторы разбиты на три класса:

- операторы сравнения: =, \diamond , <, <=, >, >=, in;
- арифметические операторы: +, -, *, /, mod, ^;
- логические операторы: not, and, or.

Пример 1:

```
gap>2*2;; #два знака ";" подавляют вывод на экран
gap>2*2+9=Fibonacci(7) and Fibonacci(13) in Prime;
true
```

Сравнения выражений

Формат:

left-expr = right-expr

left-expr \diamond right-expr

Примечание: любые объекты сравнимы между собой. Объекты различных типов всегда различны, т.е. = приведет к false, и \diamond — к true. Кроме того, для них определено отношение «меньше».

Операторы сравнения имеют больший приоритет по сравнению с логическими операторами, но меньший по сравнению с арифметическими. Например, $a*b = c$ and d интерпретируется как $((a*b)=c)$ and d). Еще один пример (сравнение, левая часть которого является выражением):

```
gap> 2 * 2 + 9 = Fibonacci(7);
true
```

Арифметические операции

Формат:

+ right-expr

- right-expr

left-expr + right-expr

left-expr - right-expr

left-expr * right-expr

eft-expr / right-expr

left-expr mod right-expr

left-expr ^ right-expr

Значение, как правило, зависит от типа операндов. Mod определен только для целых и рациональных чисел. Для элемента группы ^ означает возведение в степень, если правый операнд - целое число, а если он — также элемент группы, то сопряжение с его помощью. Приоритет операторов (по убыванию):

3) ^

4) унарные + и -

5) *, /, mod

6) + и -

Пример: $-2 \wedge -2 * 3 + 1$ означает $(-(2 \wedge (-2))) * 3 + 1$.

Арифметические операторы имеют наивысший приоритет по сравнению с операторами сравнения и логическими операторами.

Команда присваивания.

Присваивания имеют формат

var := expr;

Команда вызова процедуры.

Формат:

procedure-var();

procedure-var(arg-expr {, arg-expr});

Различие между процедурами и функциями введено для удобства, **GAP** же их не различает. Функция возвращает значение, но не производит побочных эффектов. Процедура не возвращает никакого значения, но производит какое-либо действие (например, процедуры Print, Append, Sort).

Команда IF.

Формат:

if bool-expr1 then statements1

{ elif bool-expr2 then statements2 }


```
[ else statements3 ]
```

```
fi;
```

При этом частей `elif` может быть произвольное количество или ни одной. Часть `elseif` также может отсутствовать.

Функции.

Формат:

```
function ( [ arg-ident {, arg-ident} ] )
```

```
[ local loc-ident {, loc-ident} ; ]
```

```
Statements
```

```
end
```

Пример функции, которая определяет n -е число Фибоначчи:

```
gap>fib := function ( n )
```

```
>local f1, f2, f3, i;
```

```
>f1 := 1; f2 := 1;
```

```
>for i in [3..n] do
```

```
>f3 := f1 + f2; f1 := f2; f2 := f3;
```

```
>od;
```

```
>return f2;
```

```
>end;;
```

```
gap>List( [1..10], fib );
```

```
[ 1, 1, 2, 3, 5, 8, 13, 21, 34, 55 ]
```

2.3. Команды для вычислений в алгебрах

Пусть F — поле и A — алгебра над F (кратко: A — F -алгебра). Все алгебры в GAP ассоциативны, то есть операция умножения в них ассоциативна. Любая алгебра всегда содержит нулевой элемент, который может быть получен вычитанием произвольного элемента из самого себя. Элементы поля F не рассматриваются как элементы A . Практическим обоснованием (очевидно и математическим тоже) для этого служит то, что даже если единичная матрица со-

держится в матричной алгебре A , все равно невозможно записать $1 + a$ для суммы единичной матрицы и элемента a алгебры A , так как независимо от алгебры A в **GAP** уже определено это значение как прибавление 1 ко всем позициям матрицы a . Вместо этого необходимо писать

$\text{One}(A) + a$ или

$a^0 + a$.

Родительские алгебры и подалгебры

GAP различает алгебры и подалгебры алгебр.

Каждая подалгебра принадлежит уникальной основной алгебре, которую называют родителем подалгебры. Родительская алгебра — собственный родитель. Родительские алгебры конструируются при помощи операторов `Algebra` и `UnitalAlgebra`, подалгебры конструируются при помощи операторов `Subalgebra` и `UnitalSubalgebra`. Родитель первого аргумента оператора `Subalgebra` будет родителем созданной подалгебры. Алгебраические действия, совершаемые более, чем с одной алгеброй, предполагают, что аргументы имеют общего родителя. Возьмем, например, `Centralizer`. В этом случае должно быть два аргумента: алгебра A и алгебра B , где A родительская алгебра и B — подалгебра этой родительской алгебры, или A и B — подалгебры общей родительской алгебры P . В этих случаях `Centralizer` выдает централизатор B в A , который представлен как подалгебра общей родительской алгебры алгебр A и B . Заметим, что подалгебра родительской алгебры не должна быть собственной подалгеброй. Исключением этому правилу является теоретико-множественная функция `Intersection`, которая позволяет рассматривать пересечения алгебры с различными родительскими алгебрами. Всякий раз, когда имеется две подалгебры, которые имеют различные родительские алгебры, но имеют и общую супералгебру A , можно использовать `AsSubalgebra` или `AsUnitalSubalgebra` для того, чтобы создать новые подалгебры, которые имеют общую родительскую алгебру A .

Теоретико-множественные функции для алгебр

Все теоретико-множественные функции, например, Intersection и Sizemoгут быть применены к алгебрам, так как они являются областями. Все теоретико-множественные функции, не упомянутые здесь, не трактуются специально для алгебр.

Elements(A) вычисляет элементы алгебры A с использованием алгоритма Dimino. Заданная по умолчанию для алгебр функция вычисляет базис линейного пространства в то же самое время.

Intersection(A, H) выдает пересечение A и H в виде множества элементов или как алгебраическую запись(записьалгебры).

IsSubset (A, H)

Если A и H — алгебры, то IsSubset проверяет являются ли генераторы H элементами A. Другой способ состоит в применении DomainOps.IsSubset.

Random(A) выдает произвольный элемент алгебры A. Это требует вычисления базиса линейного пространства.

Проверка свойств алгебр

С помощью GAPA могут быть проверены следующие свойства алгебр.

IsAbelian(A) выдается true если алгебра A абелева и false в противном случае. Алгебра A называется абелевой, если и только, если для любых $a, b \in A$ $a*b = b*a$.

IsCentral(A, U) выдает true если алгебра A централизует алгебру U и false в противном случае. Алгебра A централизует алгебру U, если и только, если для всякого $a \in A$ и для всякого $u \in U$ $a*u = u*a$. Заметьте, что U не обязана быть подалгебройA, но онидолжны иметь общую родительскую алгебру.

IsFinite(A) выдает true если алгебра A конечна, и false в противном случае.

IsTrivial(A) выдает true если алгебра A состоит только из нулевого элемента, и false в противном случае. Если A — унитарная алгебра, то, конечно, она никогда не тривиальна.

Все критерии ожидают родительскую алгебру или подалгебру и выдают true, если алгебра имеет свойство и false в противном случае. Некоторые функ-

ции не могут выполняться, если данная алгебра имеет бесконечное множество элементов. В таких случаях может быть напечатано предупреждение.

Функции линейного пространства для алгебр

Конечномерная F - алгебра Всегда есть конечномерное векторное пространство над F . Таким образом, в **GAPe**, алгебра — линейное пространство, и функции линейного пространства типа `Base` и `Dimension` применимы к алгебрам.

Структура линейного пространства используется также теоретико-множественными функциями.

Алгебраические функции для алгебр

Функции, описанные в этом разделе, вычисляют некоторые подалгебры данной алгебры, например, `Centre` вычисляет центр алгебры. Некоторые функции не могут завершиться, если данная алгебра имеет бесконечное множество элементов, в то время как другие функции могут сообщить об ошибке в таких случаях.

В **GAPe** каждая алгебра является или родительской алгеброй или подалгеброй единственной родительской алгебры. Если Вы вычисляете центр C алгебры U с родительской алгеброй A , то C — подалгебра U , но ее родительская алгебра есть A .

ГЛАВА III. Типовая классификация трехмерных подалгебр алгебры матриц $M(GF(2), 3)$

3.1. Трехмерные подалгебры алгебры матриц над полем из двух элементов

Теорема 1. В алгебре квадратных матриц третьего порядка над полем из двух элементов содержится 736 трехмерных подалгебр.

Доказать эту теорему можно при помощи программы, написанной в **GAP**, которая считает количество подалгебр трехмерных алгебр над полем из двух элементов:

Программа №1		
№	Текст программы	Комментарии
1	<code>Ssub:=[];</code>	Создаем массив для
2	<code>Sub:=[];b:=0;</code>	Создание массива sub и переменной b
3	<code>A:=MatAlgebra(GF(2),3);</code>	Построение алгебры матриц третьего порядка над полем GF(2)
4	<code>El:=Elements(A);</code>	Создание массива элементов алгебры A
5	<code>for i in [1..512] do</code>	Начало цикла
6	<code>for k in [i..512] do</code>	Начало цикла
7	<code>for j in [k..512] do</code>	Начало цикла
8	<code>B:=Subalgebra(A,[El[i],El[k],El[j]]);</code>	Записывает подалгебру алгебры A порожденную элементом El[i], El[k], El[j] в B
9	<code>sub:=Elements(B);</code>	Кладем в массив sub элементы подалгебры B
10	<code>if Size(sub)=8 then</code>	Проверяем размер массива sub. Если равен 8
11	<code>AddSet(Sub,sub);</code>	То записываем его в массив Sub

12	<i>if Size(Sub) > b then</i>	Сравниваем размер массива Sub с b. Если размер больше
13	<i>Add(Ssub, [i, k, j]);</i>	То записываем в массив E1E2E2RRE10
14	<i>b:=Size(Sub);</i>	Присваиваем b размер массива sub
15	<i>fi;</i>	Конец цикла
16	<i>fi;</i>	Конец цикла
17	<i>od;</i>	Конец цикла
18	<i>od;</i>	Конец цикла
19	<i>od;</i>	Конец цикла
20	<i>PrintTo("trehm_pod1.dan", "Ssub :=", Ssub, ";", "\n", " Ssub =", Size(Ssub), "\n");</i>	Печатаем массив Ssub в файл trehm_pod1.dan

Теорема 2. В алгебре квадратных матриц третьего порядка над полем из двух элементов содержится 736 трехмерных подалгебры, которые образуют 9 различных типов подалгебр. Приведём их описание в следующей таблице:

Таблица №2

№	Тип решетки	Число подалгебр в подалгебре данного типа	Моногенные	Количество подалгебр данного типа	Количество подалгебр данной размерности
1	(1,1,1)	3	+	8	736
2	(1,2,2,1)	6	+	21	
3	(1,3,2,1)	7	+	28	
4	(1,4,4,1)	10	-	98	
5	(1,5,3,1)	10	-	21	
6	(1,5,4,1)	11	-	168	
7	(1,6,5,1)	13	-	336	

8	(1,7,6,1)	15	-	28	
9	(1,7,7,1)	16	-	28	

Доказательство данной теоремы приводится в дипломной работе Гришиной А.А. Подалгебры матричной алгебры $M_3(GF(2))$.

Теорема 3. В алгебре квадратных матриц третьего порядка над полем из двух элементов содержится всего 679 немоногенных трехмерных подалгебр, которые образуют 6 попарно различных типов подалгебр. Приведём их полное описание в следующей таблице:

Таблица №3

№	Порождающие элементы	Определяющие соотношения	Количество подалгебр	Тип решетки подалгебр
1	e_1, e_2, r	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j$, $e_1 r = r e_1 = 0, e_2 r = r e_2 = r$	84	(1,4,4,1)
2	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, e r_1 = r_1 e = r_1,$ $e r_2 = r_2 = r_2 e$	14	(1,4,4,1)
3	r_1, r_2	$r_1^3 = 0, r_1^2 \neq 0, r_2^2 = 0, r_1 r_2 = r_1^2,$ $r_2 r_1 = 0$	21	(1,5,3,1)
4	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, e r_1 = r_1 e = 0,$ $e r_2 = r_2, r_2 e = 0$	42	(1,5,4,1)
5	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, e r_1 = r_1 e = 0,$ $e r_2 = 0, r_2 e = r_2$	42	(1,5,4,1)
6	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, e r_1 = r_1 e = r_1,$	42	(1,5,4,1)

		$er_2 = r_2, r_2e = 0$		
7	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, er_1 = r_1 e$ $= r_1,$ $er_2 = 0, r_2 e = r_2$	42	(1,5,4,1)
8	e_1, e_2, r	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j,$ $e_1 r = r e_1 = 0, e_2 r = 0, r e_2 = r$	84	(1,6,5,1)
9	e_1, e_2, r	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j,$ $e_1 r = r e_1 = 0, e_2 r = r, r e_2 = 0$	84	(1,6,5,1)
10	e_1, e_2, r	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j,$ $e_2 r = r e_1 = 0, e_1 r = r = r e_2$	168	(1,6,5,1)
11	e_1, e_2, e_3	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j$	28	(1,7,6,1)
12	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, er_i = 0,$ $r_i e = r_i$	14	(1,7,7,1)
13	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, r_i e = 0,$ $er_i = r_i$	14	(1,7,7,1)
		ИТОГО:	679	6

Теорема 4. Подалгебра S алгебры A тогда и только тогда имеет тип решетки $(1, 4, 4, 1)$, когда S изоморфна одной из следующих подалгебр:

Таблица №4

По- да- лг- еб- ра	Порожда- ющие эле- менты	Определяющие соотношения	Количество подалгебр	Тип решетки подалгебр
S_I	e_1, e_2, r	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j,$ $e_1 r = r e_1 = 0, e_2 r = r e_2 = r$	84	(1,4,4,1)

S_2	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, er_1 = r_1 e$ $= r_1,$ $er_2 = r_2 = r_2 e$	14	(1,4,4,1)
-------	---------------	--	----	-----------

Доказательство можно провести с помощью следующей программы:

Программа №2		
№	Текст программы	Комментарии
1	$ERROR := [] ;$	Создаем массив
2	$Sub := [] ; b := 0 ;$	Создание массива sub и переменной b
3	$NI := [3, 5, 7, 9, 28, 33, 37,$ $41, 64, 65, 73, 129, 131,$ $193, 220, 326, 366, 433, 439,$ $456, 505] ;$	Массив номеров 2-нильпотентных матриц
4	$ID := [2, 4, 6, 8, 10, 17, 18,$ $19, 22, 25, 46, 49, 50, 54,$ $55, 57, 66, 74, 82, 122, 145,$ $146, 147, 152, 196, 210, 217,$ $239, 257, 258, 260, 261, 266,$ $273, 274, 275, 277, 279, 281,$ $289, 290, 293, 296, 298, 317,$ $321, 337, 345, 361, 385, 386,$ $388, 391, 449, 458, 467, 512$ $] ;$	Массив номеров идемпотентных матриц
5	$A := MatAlgebra (GF(2), 3) ;$	Построение алгебры матриц третьего порядка над полем GF(2)
6	$El := Elements (A) ;$	Создание массива элементов алгебры A
7	$for\ i\ in\ ID\ do$	Начало цикла
8	$for\ k\ in\ ID\ do$	Начало цикла
9	$for\ j\ in\ NI\ do$	Начало цикла
10	$if\ El[i] * El[k] = El[1]\ and$ $El[k] * El[i] = El[1]$	Условия
11	$and\ El[i] * El[j] = El[1]\ and$ $El[j] * El[i] = El[1]$	

12	$and \quad El[j] * El[k] = El[j] \quad and$ $El[k] * El[j] = El[j]$	
13	$then$	
14	$B := Subalgebra$ $(A, [El[i], El[k], El[j]]);$	Записывает подалгебру- алгебры порожденную элементами $El[i], El[k],$ $El[j]$ в B
15	$sub := Elements(B);$	Кладем в массив sub элементы подалгебры B
16	$if Size(sub) = 8 \quad then$	Проверяем размер мас- сива sub . Если равен 8
17	$AddSet(Sub, sub);$	То записываем его в массив Sub
18	$if Size(Sub) > b \quad then$	Сравниваем размер мас- сива Sub с b . Если раз- мер больше
19	$Add(E1E2E2RRE10, [i, k, j]);$	То записываем в массив $E1E2E2RRE10$
20	$b := Size(Sub);$	Присваиваем b размер массива sub
21	$fi;$	Конец цикла
22	$fi;$	Конец цикла
23	$fi;$	Конец цикла
24	$od;$	Конец цикла
25	$od;$	Конец цикла
26	$od;$	Конец цикла
27	$Sort(EER0R);$	Упорядочиваем элементы массива $EER0R$
28	$PrintTo("3eer=0r.dan", "EER0R:$ $=",$ $EER0R, ";", "\n", " EER0R =", Size$ $e(EER0R), "\n");$	Печатаем массив $EER0R$ в файл $3eer=0r.dan$

Замечание. Приведенная программа строит подалгебру S_1 . Программа для построения подалгебры S_2 отличается в строках 10-12:

S_1	S_2
$El[i] * El[k] = El[1] \text{ and}$ $El[k] * El[i] = El[1]$	$El[i] * El[k] = El[k] \text{ and}$ $El[k] * El[i] = El[k]$
$\text{and } El[i] * El[j] = El[1] \text{ and}$ $El[j] * El[i] = El[1]$	$\text{and } El[i] * El[j] = El[j] \text{ and}$ $El[j] * El[i] = El[j]$
$\text{and } El[j] * El[k] = El[j] \text{ and}$ $El[k] * El[j] = El[j]$	$\text{and } El[j] * El[k] = El[1] \text{ and}$ $El[k] * El[j] = El[1]$

Результатами программ являются массивы номеров троек базисных элементов.

EER0R:= [[2, 273, 33], [2, 273, 129], [2, 273, 433], [4, 275, 37], [4, 275, 129], [4, 275, 439], [6, 277, 33], [6, 277, 131], [6, 277, 439], [8, 279, 37], [8, 279, 131], [8, 279, 433], [10, 281, 33], [10, 281, 193], [10, 281, 505], [17, 258, 5], [17, 258, 65], [17, 258, 326], [19, 260, 5], [19, 260, 193], [19, 260, 456], [25, 266, 37], [25, 266, 65], [25, 266, 366], [46, 317, 33], [46, 317, 220], [46, 317, 456], [49, 290, 5], [49, 290, 73], [49, 290, 366], [55, 296, 5], [55, 296, 220], [55, 296, 505], [57, 298, 37], [57, 298, 73], [57, 298, 326], [66, 337, 41], [66, 337, 129], [66, 337, 505], [74, 345, 41], [74, 345, 193], [74, 345, 433], [145, 386, 7], [145, 386, 65], [145, 386, 456], [147, 388, 7], [147, 388, 193], [147, 388, 326], [196, 467, 64], [196, 467, 129], [196, 467, 366], [217, 458, 64], [217, 458, 65], [217, 458, 439], [257, 18, 3], [257, 18, 9], [257, 18, 28], [261, 22, 3], [261, 22, 41], [261, 22, 64], [289, 50, 7], [289, 50, 9], [289, 50, 64], [293, 54, 7], [293, 54, 28], [293, 54, 41], [321, 82, 9], [321, 82, 131], [321, 82, 220], [361, 122, 9], [361, 122, 439], [361, 122, 456], [385, 146, 3], [385, 146, 73], [385, 146, 220], [391, 152, 3], [391, 152, 366], [391, 152, 505], [449, 210, 28], [449, 210, 73], [449, 210, 131], [512, 239, 28], [512, 239, 326], [512, 239, 433]];

$$|EER0R|=84$$

ERRR:= [[274, 3, 5], [274, 3, 129], [274, 5, 33], [274, 7, 433], [274, 9, 33], [274, 9, 65], [274, 28, 37], [274, 28, 193], [274, 41, 326], [274, 64, 456], [274, 65, 129], [274, 73, 433], [274, 131, 326], [274, 220, 366]];

$$|ERRR|=14$$

Доказательство следующих теорем осуществляется с помощью программ, аналогичных программе №2. Отличия этих программ состоят в блоках, задающих умножения в соответствующей алгебре.

Теорема 5. *Подалгебра S алгебры A тогда и только тогда имеет тип решетки $(1, 5, 3, 1)$, когда S изоморфна следующей подалгебре S_3 :*

Таблица №5

По- да- лг- еб- ра	Порожда- ющие эле- менты	Определяющие соотношения	Количество подалгебр	Тип решетки подалгебр
S_3	r_1, r_2	$r_1^3 = 0, r_1^2 \neq 0, r_2^2 = 0, r_1 r_2 = r_1^2,$ $r_2 r_1 = 0$	21	(1,5,3,1)

Получен результат в виде массива номеров троек базисных элементов.

RR:= [[13, 5], [32, 5], [35, 33], [67, 3], [79, 7], [92, 28], [97, 65], [120, 64], [133, 129], [137, 9], [171, 41], [190, 64], [222, 7], [229, 193], [244, 41], [328, 3], [334, 326], [375, 28], [435, 433], [441, 9], [477, 456]];

|RR|=21

Теорема 6. *Подалгебра S алгебры A тогда и только тогда имеет тип решетки $(1, 5, 4, 1)$, когда S изоморфна одной из следующих подалгебр:*

Таблица №6

По- да- лг- еб- ра	Порожда- ющие эле- менты	Определяющие соотношения	Количество подалгебр	Тип решетки подалгебр
S_I	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, e r_1 = r_1 e$ $= 0,$	42	(1,5,4,1)

		$er_2 = r_2, r_2e = 0$		
S_2	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, er_1 = r_1 e$ $= 0,$ $er_2 = 0, r_2 e = r_2$	42	(1,5,4,1)
S_3	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, er_1 = r_1 e$ $= r_1,$ $er_2 = r_2, r_2 e = 0$	42	(1,5,4,1)
S_4	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, er_1 = r_1 e$ $= r_1,$ $er_2 = 0, r_2 e = r_2$	42	(1,5,4,1)

Результатами программ являются массивы номеров троек базисных элементов.

RER0RER:= [[3, 257, 5], [3, 385, 7], [5, 17, 3], [5, 49, 7], [7, 145, 3], [7, 289, 5], [9, 257, 33], [9, 321, 41], [28, 257, 37], [28, 449, 64], [33, 2, 9], [33, 6, 41], [37, 4, 28], [37, 8, 64], [41, 66, 9], [41, 261, 33], [64, 196, 28], [64, 261, 37], [65, 17, 129], [65, 25, 193], [73, 49, 433], [73, 57, 505], [129, 2, 65], [129, 4, 193], [131, 6, 326], [131, 8, 456], [193, 10, 65], [193, 19, 129], [220, 46, 366], [220, 55, 439], [326, 17, 131], [326, 57, 456], [366, 25, 220], [366, 49, 439], [433, 2, 73], [433, 8, 505], [439, 4, 220], [439, 6, 366], [456, 19, 131], [456, 46, 326], [505, 10, 73], [505, 55, 433]];

|RER0RER|=42

RERRRE0:= [[3, 257, 129], [3, 261, 131], [5, 17, 33], [5, 19, 37], [7, 145, 433], [7, 147, 439], [9, 257, 65], [9, 289, 73], [28, 257, 193], [28, 293, 220], [33, 2, 5], [33, 10, 37], [37, 4, 5], [37, 25, 33], [41, 66, 326], [41, 74, 366], [64, 196, 456], [64, 217, 505], [65, 17, 9], [65, 145, 73], [73, 49, 9], [73, 385, 65], [129, 2, 3], [129, 66, 131], [131, 6, 3], [131, 321, 129], [193, 10, 28], [193, 74, 220], [220, 46, 28], [220, 321, 193], [326, 17, 41], [326, 147, 366], [366,

25, 41], [366, 196, 326], [433, 2, 7], [433, 74, 439], [439, 4, 7], [439, 217, 433], [456, 19, 64], [456, 145, 505], [505, 10, 64], [505, 66, 456]];

$$|RERRRE0|=42$$

$ER1R1ER1R2e0 := [[18, 3, 5], [18, 9, 33], [18, 28, 37], [22, 41, 33], [22, 64, 37], [50, 7, 5], [82, 9, 41], [82, 131, 326], [82, 220, 366], [122, 439, 366], [122, 456, 326], [146, 3, 7], [146, 73, 433], [146, 220, 439], [152, 366, 439], [152, 505, 433], [210, 28, 64], [210, 73, 505], [210, 131, 456], [239, 326, 456], [239, 433, 505], [258, 5, 3], [258, 65, 129], [258, 326, 131], [260, 193, 129], [260, 456, 131], [266, 37, 28], [266, 65, 193], [266, 366, 220], [273, 33, 9], [273, 129, 65], [273, 433, 73], [275, 129, 193], [275, 439, 220], [277, 33, 41], [279, 37, 64], [281, 193, 65], [281, 505, 73], [290, 5, 7], [337, 41, 9], [386, 7, 3], [458, 64, 28]];$

$$|ER1R1ER1R2e0|=42$$

$ER1R1ER1 := [[18, 3, 129], [18, 9, 65], [18, 28, 193], [22, 3, 131], [22, 41, 326], [22, 64, 456], [50, 7, 433], [50, 9, 73], [50, 64, 505], [54, 7, 439], [54, 28, 220], [54, 41, 366], [82, 131, 129], [82, 220, 193], [122, 439, 433], [122, 456, 505], [146, 73, 65], [152, 366, 326], [152, 505, 456], [239, 326, 366], [239, 433, 439], [258, 5, 33], [258, 65, 9], [258, 326, 41], [260, 5, 37], [260, 193, 28], [260, 456, 64], [266, 37, 33], [266, 366, 41], [273, 33, 5], [273, 129, 3], [273, 433, 7], [275, 37, 5], [275, 439, 7], [277, 131, 3], [281, 33, 37], [281, 505, 64], [290, 73, 9], [296, 220, 28], [337, 129, 131], [345, 193, 220], [386, 65, 73]];$

$$|ER1R1ER1|=42$$

Теорема 7. Подалгебра S алгебры A тогда и только тогда имеет тип решетки $(1, 6, 5, 1)$, когда S изоморфна одной из следующих подалгебр:

Таблица №7

По да	Порождающие эле-	Определяющие соотношения	Количество подалгебр	Тип решетки подалгебр
-------	------------------	--------------------------	----------------------	-----------------------

ЛГ еб ра	МЕНТЫ			
S_1	e_1, e_2, r	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j$, $e_1 r = r e_1 = 0, e_2 r = 0, r e_2 = r$	84	(1,6,5,1)
S_2	e_1, e_2, r	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j$, $e_1 r = r e_1 = 0, e_2 r = r, r e_2 = 0$	84	(1,6,5,1)
S_3	e_1, e_2, r	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j$, $e_2 r = r e_1 = 0, e_1 r = r = r e_2$	168	(1,6,5,1)

Результатами программ являются массивы номеров троек базисных элементов.

E1E2E2RRE10:= [[2, 17, 3], [2, 49, 7], [2, 145, 3], [2, 257, 5], [2, 273, 3], [2, 273, 5], [2, 273, 7], [2, 289, 5], [2, 385, 7], [4, 55, 7], [4, 257, 5], [4, 275, 5], [4, 275, 7], [4, 293, 5], [4, 385, 7], [6, 17, 3], [6, 147, 3], [6, 277, 3], [10, 25, 28], [10, 57, 64], [10, 217, 28], [10, 257, 37], [10, 281, 28], [10, 281, 37], [10, 281, 64], [10, 289, 37], [10, 449, 64], [17, 2, 9], [17, 6, 41], [17, 66, 9], [17, 257, 33], [17, 258, 9], [17, 258, 33], [17, 258, 41], [17, 261, 33], [17, 321, 41], [18, 257, 5], [18, 257, 33], [18, 257, 37], [19, 8, 64], [19, 257, 37], [19, 260, 37], [19, 260, 64], [19, 261, 37], [19, 449, 64], [22, 261, 33], [22, 261, 37], [25, 46, 41], [25, 257, 33], [25, 266, 33], [25, 266, 41], [25, 293, 33], [25, 321, 41], [46, 25, 28], [46, 196, 28], [46, 317, 28], [49, 2, 9], [49, 74, 9], [49, 290, 9], [50, 289, 5], [66, 17, 131], [66, 57, 456], [66, 145, 131], [66, 321, 326], [66, 337, 131], [66, 337, 326], [66, 337, 456], [66, 361, 326], [66, 449, 456], [74, 25, 220], [74, 49, 439], [74, 217, 220], [74, 321, 366], [74, 345, 220], [74, 345, 366], [74, 345, 439], [74, 361, 366], [74, 385, 439], [82, 321, 41], [82, 321, 326], [82, 321, 366], [122, 361, 326], [122, 361, 366], [145, 2, 73], [145, 8, 505], [145, 66, 73], [145, 385, 433], [145, 386, 73], [145, 386, 433], [145,

386, 505], [145, 391, 433], [145, 449, 505], [146, 385, 7], [146, 385, 433], [146, 385, 439], [147, 6, 366], [147, 321, 366], [147, 385, 439], [147, 388, 366], [147, 388, 439], [147, 391, 439], [152, 391, 433], [152, 391, 439], [196, 46, 326], [196, 321, 326], [196, 449, 456], [196, 467, 326], [196, 467, 456], [196, 512, 456], [210, 449, 64], [210, 449, 456], [210, 449, 505], [217, 55, 433], [217, 385, 433], [217, 449, 505], [217, 458, 433], [217, 458, 505], [217, 512, 505], [239, 512, 456], [239, 512, 505], [257, 2, 65], [257, 4, 193], [257, 10, 65], [257, 17, 129], [257, 18, 65], [257, 18, 129], [257, 18, 193], [257, 19, 129], [257, 25, 193], [258, 17, 3], [258, 17, 129], [258, 17, 131], [260, 19, 129], [260, 19, 131], [261, 17, 131], [261, 19, 131], [261, 22, 131], [266, 25, 28], [266, 25, 193], [266, 25, 220], [273, 2, 9], [273, 2, 65], [273, 2, 73], [275, 4, 193], [275, 4, 220], [277, 6, 41], [279, 8, 64], [281, 10, 65], [281, 10, 73], [289, 2, 73], [289, 10, 73], [289, 50, 73], [290, 49, 7], [293, 4, 220], [293, 25, 220], [293, 54, 220], [321, 17, 129], [321, 25, 193], [321, 82, 129], [321, 82, 193], [321, 147, 129], [321, 196, 193], [337, 66, 9], [385, 2, 65], [385, 74, 65], [385, 146, 65], [386, 145, 3], [458, 217, 28]];

|E1E2E2RRE10|=168

EER0RER:= [[2, 17, 129], [2, 49, 433], [2, 257, 33], [4, 19, 129], [4, 55, 439], [4, 257, 37], [6, 17, 131], [6, 49, 439], [6, 261, 33], [8, 19, 131], [8, 55, 433], [8, 261, 37], [10, 25, 193], [10, 57, 505], [10, 257, 33], [17, 2, 65], [17, 6, 326], [17, 257, 5], [19, 4, 193], [19, 8, 456], [19, 257, 5], [25, 10, 65], [25, 46, 366], [25, 257, 37], [46, 25, 220], [46, 57, 456], [46, 261, 33], [49, 2, 73], [49, 6, 366], [49, 289, 5], [55, 4, 220], [55, 8, 505], [55, 289, 5], [57, 10, 73], [57, 46, 326], [57, 261, 37], [66, 17, 129], [66, 57, 505], [66, 321, 41], [74, 25, 193], [74, 49, 433], [74, 321, 41], [145, 2, 65], [145, 8, 456], [145, 385, 7], [147, 4, 193], [147, 6, 326], [147, 385, 7], [196, 19, 129], [196, 46, 366], [196, 449, 64], [217, 10, 65], [217, 55, 439], [217, 449, 64], [257, 2, 9], [257, 4, 28], [257, 17, 3], [261, 6, 41], [261, 8, 64], [261, 17, 3], [289, 2, 9], [289, 8, 64], [289, 49, 7], [293, 4, 28], [293, 6, 41], [293, 49, 7], [321, 17, 131], [321, 25, 220]

, [321, 66, 9], [361, 49, 439], [361, 57, 456], [361, 66, 9], [385, 2, 73], [385, 4, 220], [385, 145, 3], [391, 6, 366], [391, 8, 505], [391, 145, 3], [449, 10, 73], [449, 19, 131], [449, 196, 28], [512, 46, 326], [512, 55, 433], [512, 196, 28]];

$$|EER0RER|=84$$

EERRRE0:= [[2, 17, 33], [2, 145, 433], [2, 257, 129], [4, 19, 37], [4, 147, 439], [4, 257, 129], [6, 17, 33], [6, 147, 439], [6, 261, 131], [8, 19, 37], [8, 145, 433], [8, 261, 131], [10, 25, 33], [10, 217, 505], [10, 257, 193], [17, 2, 5], [17, 66, 326], [17, 257, 65], [19, 4, 5], [19, 196, 456], [19, 257, 193], [25, 10, 37], [25, 74, 366], [25, 257, 65], [46, 25, 33], [46, 196, 456], [46, 293, 220], [49, 2, 5], [49, 74, 366], [49, 289, 73], [55, 4, 5], [55, 217, 505], [55, 293, 220], [57, 10, 37], [57, 66, 326], [57, 289, 73], [66, 17, 41], [66, 145, 505], [66, 321, 129], [74, 25, 41], [74, 217, 433], [74, 321, 193], [145, 2, 7], [145, 66, 456], [145, 385, 65], [147, 4, 7], [147, 196, 326], [147, 321, 193], [196, 19, 64], [196, 147, 366], [196, 321, 129], [217, 10, 64], [217, 74, 439], [217, 385, 65], [257, 2, 3], [257, 10, 28], [257, 17, 9], [261, 6, 3], [261, 17, 41], [261, 19, 64], [289, 2, 7], [289, 10, 64], [289, 49, 9], [293, 4, 7], [293, 25, 41], [293, 46, 28], [321, 17, 9], [321, 66, 131], [321, 74, 220], [361, 49, 9], [361, 66, 456], [361, 74, 439], [385, 2, 3], [385, 74, 220], [385, 145, 73], [391, 6, 3], [391, 145, 505], [391, 147, 366], [449, 10, 28], [449, 66, 131], [449, 145, 73], [512, 46, 28], [512, 196, 326], [512, 217, 433]];

$$|EERRRE0|=84$$

Теорема 8. *Подалгебра S алгебры A тогда и только тогда имеет тип решетки $(1, 7, 6, 1)$, когда S изоморфна следующей подалгебре:*

Таблица №8

По- да- лг- еб	Порожда- ющие эле- менты	Определяющие соотношения	Количество подалгебр	Тип решетки подалгебр

ра				
S_I	e_1, e_2, e_3	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i = j$	28	(1,7,6,1)

Получен результат в виде массива номеров троек базисных элементов.

EEE0:= [[2, 17, 257], [2, 49, 289], [2, 145, 385], [4, 19, 257], [4, 55, 293], [4, 147, 385], [6, 17, 261], [6, 49, 293], [6, 147, 391], [8, 19, 261], [8, 55, 289], [8, 145, 391], [10, 25, 257], [10, 57, 289], [10, 217, 449], [17, 66, 321], [19, 196, 449], [25, 46, 293], [25, 74, 321], [46, 57, 261], [46, 196, 512], [49, 74, 361], [55, 217, 512], [57, 66, 361], [66, 145, 449], [74, 217, 385], [147, 196, 321], [361, 391, 512]];

$$|EEE0|=28$$

Теорема 9. Подалгебра S алгебры A тогда и только тогда имеет тип решетки (1, 7, 7, 1), когда S изоморфна одной из следующих подалгебр:

Таблица №9

По- да- лг- еб- ра	Порожда- ющие эле- менты	Определяющие соотношения	Количество подалгебр	Тип решетки подалгебр
S_1	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, e r_i = 0,$ $r_i e = r_i$	14	(1,7,7,1)
S_2	r_1, r_2, e	$r_i r_j = r_j r_i = 0, e^2 = e, r_i e = 0,$ $e r_i = r_i$	14	(1,7,7,1)

Результатами программ являются массивы номеров троек базисных элементов.

ERR0RRER:= [[2, 9, 65], [4, 28, 193], [6, 41, 326], [8, 64, 456], [17, 3, 129], [18, 65, 129], [22, 131, 326], [49, 7, 433], [50, 73, 433], [54, 220, 366], [257, 5, 33], [258, 9, 33], [260, 28, 37], [273, 3, 5]];

|ERR0RRER|=14

ERRRRRE0:= [[2, 3, 5], [10, 28, 37], [17, 9, 33], [18, 5, 33], [66, 131, 326], [74, 220, 366], [82, 41, 326], [145, 73, 433], [146, 7, 433], [210, 64, 456], [257, 65, 129], [258, 3, 129], [266, 28, 193], [273, 9, 65]];

|ERRRRRE0|=14

3.2. Вычисление типов решеток подалгебр

Типы решеток подалгебр были найдены по следующей программе:

Программа №3	
<i>tip:=function(a,b,c)</i>	Задаем функцию
<i>local</i>	Создаем локальные переменные
<i>A,El,i,j, k,sub, tip,S,s, el,l;</i>	Имена переменных
<i>sub:=[];</i>	Задаем пустой массив sub
<i>tip:=[];</i>	Задаем пустой массив tip
<i>A:=MatAlgebra(GF(2),3);</i>	Создание алгебры матриц
<i>El:=Elements(A);</i>	Построение массива элементов
<i>S:=Subalgebra(A,[El[a],El[b],El[c]]);</i>	Построение подалгебры
<i>for i in S do</i>	Начало цикла
<i>for k in S do</i>	Начало цикла
<i>for j in S do</i>	Начало цикла
<i>s:=Subalgebra(A,[i,j,k]);</i>	Построение подалгебры
<i>AddSet(sub,Elements(s));</i>	Построение массива элементов и добавление его в массив sub
<i>od;</i>	Заккрытие цикла
<i>od;</i>	Заккрытиецикла
<i>od;</i>	Заккрытиецикла
<i>for l in [1..Size(sub)] do</i>	Начало цикла
<i>Add(tip,Size(sub[l]));</i>	Добавление порядка каждо-

	го элемента в массив <code>tip</code>
<code>od;</code>	Заккрытие цикла
<code>tip:=Collected(tip);</code>	Считаем количество элементов каждого порядка и сохраняем их в <code>tip</code>
<code>PrintTo("tip.txt","a=",a,";", " b= ",b,";", " c= ",c,";", "\n",tip);</code>	Распечатываем результаты в файл <code>tip.txt</code>
<code>end;;</code>	Конец функции

На примере программы № 2 после запуска программы № 3 зададим в **GAP** типодной из подалгебр, которые выдала первая программа: `tip(2, 273, 33)`.

Программа распечатала `[[1, 1], [2, 4], [4, 4], [8, 1]]`, где

`[1, 1]` – одна подалгебра порядка 1, то есть нулевая подалгебра;

`[2, 4]` – 4 подалгебры порядка 2;

`[4, 4]` – 4 подалгебры порядка 4;

`[8, 1]` – 1 подалгебра порядка 8.

Полученную последовательность пар можно переписать и в таком виде (1, 4, 4, 1).

С помощью данной программы вычисляется тип подалгебры для каждого определяющего соотношения.

3.3. *Выяснение отношения покрытия на множестве подалгебр*

Для построения решеток необходимо выяснить отношение покрытия с помощью следующей программы:

Программа №4	
<code>pokr:=function(a,b,c)</code>	Задание функции
<code> local</code>	Задание переменных
<code> A,El,i,j,k,sub,</code> <code> tip,S,s,s1, el,l,</code> <code> l1, m,m1,n,n1,i1;</code>	Имена переменных
<code>sub:=[];</code>	Создаем массив <code>sub</code>
<code>for i1 in [1..9] do</code>	Начало цикла
<code>sub[i1]:=[];</code>	Создаем в массиве <code>sub</code> 9 пустых

	массивов
<i>od;</i>	Конец цикла
<i>pokr:=[];</i>	Создание массива pokr
<i>A:=MatAlgebra(GF(2),3);</i>	Создание алгебры
<i>El:=Elements(A);</i>	Построение массива элементов
<i>S:=Subalgebra(A,[El[a],El[b],El[c]]);</i>	Записывает подалгебру алгебры A порожденную элементами El[a], El[b], El[c] в S
<i>for i in S do</i>	Начало цикла
<i>for k in S do</i>	Начало цикла
<i>for j in S do</i>	Начало цикла
<i>s1:=Subalgebra(S,[i,k,j]);</i>	Записывает подалгебру алгебры S порожденную элементами i, k, j в s1
<i>if Size(s1)=1 then</i>	Проверяем размер. Если равен 1
<i>AddSet(sub[1],Elements(s1));</i>	Записываем в 1-й массив
<i>fi;</i>	Закрываем проверку условия
<i>if Size(s1)=2 then</i>	Если равен 2
<i>AddSet(sub[2],Elements(s1));</i>	Записываем во 2-й массив
<i>fi;</i>	Закрываем проверку условия
<i>if Size(s1)=4 then</i>	Если равен 4
<i>AddSet(sub[3],Elements(s1));</i>	Записываем в 3-й массив
<i>fi;</i>	Закрываем проверку условия
<i>if Size(s1)=8 then</i>	Если равен 8
<i>AddSet(sub[4],Elements(s1));</i>	Записываем в 4-й массив
<i>fi;</i>	Закрываем проверку условия
<i>if Size(s1)=16 then</i>	Если равен 16
<i>AddSet(sub[5],Elements(s1));</i>	Записываем в 5-й массив
<i>fi;</i>	Закрываем проверку условия
<i>if Size(s1)=32 then</i>	Если равен 32
<i>AddSet(sub[6],Elements(s1));</i>	Записываем в 6-й массив
<i>fi;</i>	Закрываем проверку условия
<i>if Size(s1)=64 then</i>	Проверяем размер. Если равен 64
<i>AddSet(sub[7],Elements(s1));</i>	Записываем в 7-й массив

<code>));</code>	
<code>fi;</code>	Закрываем проверку условия
<code>if Size(s1)=128 then</code>	Если равен 128
<code>AddSet(sub[8],Elements(s1));</code>	Записываем в 8-й массив
<code>fi;</code>	Закрываем проверку условия
<code>if Size(s1)=512 then</code>	Проверяем размер. Если равен 512
<code>AddSet(sub[9],Elements(s1));</code>	Записываем в 9-й массив
<code>fi;</code>	Закрываем проверку условия
<code>od;</code>	Заккрытие цикла
<code>od;</code>	Заккрытие цикла
<code>od;</code>	Заккрытие цикла
<code>for m1 in [1..Size(sub)] do</code>	Открытие цикла
<code>for l1 in [1..Size(sub[m1])] do</code>	Открытие цикла
<code>for n1 in [1..Size(sub[m1+1])] do</code>	Открытие цикла
<code>if IsSub-set(sub[m1+1][n1],sub[m1][l1])=true</code>	Проверяет являются ли генераторы sub[m1][l1] элемента-ми sub[m1+1][n1],
<code>The-nAdd(pokr,[m1,l1],[m1+1,n1]);</code>	если да, то записывает в pokr
<code>fi;</code>	Заккрытие проверки условия
<code>od;</code>	Конец цикла
<code>od;</code>	Конец цикла
<code>od;</code>	Конец цикла
<code>PrintTo("pokr.txt", pokr,"\\n");</code>	Распечатываем массив pokr в файл pokr.txt
<code>end;;</code>	Конец функции

На примере программы № 2 после запуска программы № 4 зададим в **GAP** отношение покрытия одной из подалгебр, которые выдала первая программа: pokr(2, 273, 33).

В результате программа распечатает файл:

```
[[ [1, 1], [2, 1] ], [ [1, 1], [2, 2] ], [ [1, 1], [2, 3] ],
[ [1, 1], [2, 4] ], [ [2, 1], [3, 1] ], [ [2, 1], [3, 2] ],
[ [2, 2], [3, 1] ], [ [2, 2], [3, 3] ], [ [2, 2], [3, 4] ],
```

$[[2, 3], [3, 2]], [[2, 3], [3, 3]], [[2, 4], [3, 2]],$
 $[[2, 4], [3, 4]], [[3, 1], [4, 1]], [[3, 2], [4, 1]],$
 $[[3, 3], [4, 1]], [[3, 4], [4, 1]]]$.

В данной программе рассматривается подалгебра S , которая содержит 8 элементов и имеет тип $(1, 4, 4, 1)$. Значит, в ней содержится одна нулевая подалгебра, 4 двухэлементных, 4 четырех элементных и 1 восьмиэлементная подалгебра. Таким образом, все подалгебры в решетке подалгебр алгебры S распределены по четырем уровням. На каждом уровне алгебры имеют двойные номера, например, номер $[3, 2]$ означает, что 3 – номер уровня, а 2 – порядковый номер подалгебры на третьем уровне. Таким образом, запись $[[3, 2], [4, 1]]$ означает, что подалгебра с номером $[3, 2]$ покрывается подалгеброй с номером $[4, 1]$ в решетке подалгебр алгебры S .

Запустив все созданные мной программы для разных определяющих соотношений, найдя тип и отношение покрытие для полученных троек матриц, объединяем все в одну таблицу:

Таблица №10

№	Тип	Покрытие	Определяющие соотношения
1	$(1, 4, 4, 1)$	$[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]],$ $[[1, 1], [2, 4]], [[2, 1], [3, 1]], [[2, 1], [3, 2]],$ $[[2, 2], [3, 1]], [[2, 2], [3, 3]], [[2, 2], [3, 4]],$ $[[2, 3], [3, 2]], [[2, 3], [3, 3]], [[2, 4], [3, 2]],$ $[[2, 4], [3, 4]], [[3, 1], [4, 1]], [[3, 2], [4, 1]],$ $[[3, 3], [4, 1]], [[3, 4], [4, 1]]]$	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i \neq j,$ $e_1 r = r e_1 = 0, e_2 r = r e_2 = r$

2	$(1,4,4,1)$	$ \begin{aligned} &[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]]], \\ &[[1, 1], [2, 4]], [[2, 1], [3, 1]], [[2, 1], [3, 2]]], \\ &[[2, 2], [3, 1]], [[2, 2], [3, 3]], [[2, 3], [3, 1]]], \\ &[[2, 3], [3, 4]], [[2, 4], [3, 2]], [[2, 4], [3, 3]]], \\ &[[2, 4], [3, 4]], [[3, 1], [4, 1]], [[3, 2], [4, 1]]], \\ &[[3, 3], [4, 1]], [[3, 4], [4, 1]]] \end{aligned} $	$ \begin{aligned} \mathbf{r}_i \mathbf{r}_j &= \mathbf{r}_j \mathbf{r}_i = \mathbf{0}, \mathbf{e}^2 = \mathbf{e}, \mathbf{e} \mathbf{r}_1 \\ &= \mathbf{r}_1 \mathbf{e} = \mathbf{r}_1, \\ \mathbf{e} \mathbf{r}_2 &= \mathbf{r}_2 = \mathbf{r}_2 \mathbf{e} \end{aligned} $
3	$(1,5,3,1)$	$ \begin{aligned} &[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]]], \\ &[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[2, 1], [3, 1]]], \\ &[[2, 2], [3, 2]], [[2, 3], [3, 1]], [[2, 3], [3, 2]]], \\ &[[2, 3], [3, 3]], [[2, 4], [3, 1]], [[2, 5], [3, 2]]], \\ &[[3, 1], [4, 1]], [[3, 2], [4, 1]], [[3, 3], [4, 1]]] \end{aligned} $	$ \begin{aligned} \mathbf{r}_1^3 &= \mathbf{0}, \mathbf{r}_1^2 \neq \mathbf{0}, \mathbf{r}_2^2 = \mathbf{0}, \mathbf{r}_1 \mathbf{r}_2 = \mathbf{r}_1^2, \\ \mathbf{r}_2 \mathbf{r}_1 &= \mathbf{0} \end{aligned} $
4	$(1,5,4,1)$	$ \begin{aligned} &[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]]], \\ &[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[2, 1], [3, 1]]], \\ &[[2, 1], [3, 2]], [[2, 2], [3, 1]], [[2, 2], [3, 3]]], \\ &[[2, 2], [3, 4]], [[2, 3], [3, 1]], [[2, 4], [3, 2]]] \end{aligned} $	$ \begin{aligned} \mathbf{r}_i \mathbf{r}_j &= \mathbf{r}_j \mathbf{r}_i = \mathbf{0}, \mathbf{e}^2 = \mathbf{e}, \mathbf{e} \mathbf{r}_1 \\ &= \mathbf{r}_1 \mathbf{e} = \mathbf{r}_1, \\ \mathbf{e} \mathbf{r}_2 &= \mathbf{0}, \mathbf{r}_2 \mathbf{e} = \mathbf{r}_2 \end{aligned} $

		$ \begin{aligned} &], \\ &[[2, 4], [3, 3]], [[2, 5], [3, 2]], [[2, 5], [3, 4]] \\ &], \\ &[[3, 1], [4, 1]], [[3, 2], [4, 1]], [[3, 3], [4, 1]] \\ &], \\ &[[3, 4], [4, 1]]] \end{aligned} $	
5	(1,5,4,1)	$ \begin{aligned} &[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]]], \\ &[[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[2, 1], [3, 1]]], \\ &[[[2, 1], [3, 2]], [[2, 1], [3, 3]], [[2, 2], [3, 1]]], \\ &[[[2, 2], [3, 4]], [[2, 3], [3, 2]], [[2, 3], [3, 4]]], \\ &[[[2, 4], [3, 2]], [[2, 5], [3, 3]], [[2, 5], [3, 4]]], \\ &[[[3, 1], [4, 1]], [[3, 2], [4, 1]], [[3, 3], [4, 1]]], \\ &[[[3, 4], [4, 1]]] \end{aligned} $	$ \begin{aligned} \mathbf{r}_i \mathbf{r}_j &= \mathbf{r}_j \mathbf{r}_i = \mathbf{0}, \mathbf{e}^2 = \mathbf{e}, \mathbf{e} \mathbf{r}_1 \\ &= \mathbf{r}_1 \mathbf{e} = \mathbf{0}, \\ \mathbf{e} \mathbf{r}_2 &= \mathbf{r}_2, \mathbf{r}_2 \mathbf{e} = \mathbf{0} \end{aligned} $
6	(1,5,4,1)	$ \begin{aligned} &[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]]], \\ &[[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[2, 1], [3, 1]]], \\ &[[[2, 1], [3, 2]], [[2, 1], [3, 3]], [[2, 2], [3, 1]]], \\ &[[[2, 2], [3, 4]], [[2, 3], [3, 1]], [[2, 4], [3, 2]]], \\ &[[[2, 4], [3, 4]], [[2, 5], [3, 3]], [[2, 5], [3, 4]]], \\ &[[[3, 1], [4, 1]], [[3, 2], [4, 1]]] \end{aligned} $	$ \begin{aligned} \mathbf{r}_i \mathbf{r}_j &= \mathbf{r}_j \mathbf{r}_i = \mathbf{0}, \mathbf{e}^2 = \mathbf{e}, \mathbf{e} \mathbf{r}_1 \\ &= \mathbf{r}_1 \mathbf{e} = \mathbf{r}_1, \\ \mathbf{e} \mathbf{r}_2 &= \mathbf{r}_2, \mathbf{r}_2 \mathbf{e} = \mathbf{0} \end{aligned} $

		$], [4, 1]], [[3, 3], [4, 1]]$ $],$ $[[3, 4], [4, 1]]]$	
7	(1,5,4,1)	$[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]]]$ $],$ $[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[2, 1], [3, 1]]]$ $],$ $[[2, 1], [3, 2]], [[2, 1], [3, 3]], [[2, 2], [3, 1]]]$ $],$ $[[2, 2], [3, 4]], [[2, 3], [3, 2]], [[2, 3], [3, 4]]]$ $],$ $[[2, 4], [3, 2]], [[2, 5], [3, 3]], [[2, 5], [3, 4]]]$ $],$ $[[3, 1], [4, 1]], [[3, 2], [4, 1]], [[3, 3], [4, 1]]]$ $],$ $[[3, 4], [4, 1]]]$	$r_i r_j = r_j r_i = 0, e^2 = e, e r_1 = r_1 e = 0,$ $e r_2 = 0, r_2 e = r_2$
8	(1,6,5,1)	$[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]]]$ $],$ $[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]]]$ $],$ $[[2, 1], [3, 1]], [[2, 1], [3, 2]], [[2, 2], [3, 1]]]$ $],$ $[[2, 2], [3, 3]], [[2, 2], [3, 4]], [[2, 3], [3, 1]]]$ $],$ $[[2, 3], [3, 5]], [[2, 4], [3, 2]], [[2, 4], [3, 3]]]$ $],$ $[[2, 5], [3, 2]], [[2, 5], [3, 4]], [[2, 5], [3, 5]]]$ $],$ $[[2, 6], [3, 3]], [[2, 6], [3, 5]], [[3, 1], [4, 1]]]$ $],$	$e_i^2 = e_i, e_i e_j = e_j e_i = 0$ при $i \neq j,$ $e_2 r = r e_1 = 0, e_1 r = r = r e_2$

		$[[3, 2], [4, 1]], [[3, 3], [4, 1]], [[3, 4], [4, 1]],$ $[[3, 5], [4, 1]]]$	
9	(1,6,5,1)	$[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]],$ $[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]],$ $[[2, 1], [3, 1]], [[2, 1], [3, 2]], [[2, 1], [3, 3]],$ $[[2, 2], [3, 1]], [[2, 2], [3, 4]], [[2, 3], [3, 1]],$ $[[2, 3], [3, 5]], [[2, 4], [3, 2]], [[2, 4], [3, 4]],$ $[[2, 4], [3, 5]], [[2, 5], [3, 3]], [[2, 5], [3, 4]],$ $[[2, 6], [3, 3]], [[2, 6], [3, 5]], [[3, 1], [4, 1]],$ $[[3, 2], [4, 1]], [[3, 3], [4, 1]], [[3, 4], [4, 1]],$ $[[3, 5], [4, 1]]]$	$e_i^2 = e_i, e_i e_j = e_j e_i = 0 \text{ при } i = j,$ $e_1 r = r e_1 = 0, e_2 r = 0, r e_2 = r$
10	(1,6,5,1)	$[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]],$ $[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]],$ $[[2, 1], [3, 1]], [[2, 1], [3, 2]], [[2, 1], [3, 3]],$ $[[2, 2], [3, 1]], [[2, 2], [3, 4]], [[2, 3], [3, 1]],$ $[[2, 3], [3, 5]], [[2, 4], [3, 2]], [[2, 4], [3, 4]]]$	$e_i^2 = e_i, e_i e_j = e_j e_i = 0 \text{ при } i = j,$ $e_1 r = r e_1 = 0, e_2 r = r, r e_2 = 0$

		$ \begin{aligned} &], \\ &[[2, 4], [3, 5]], [[2, 5], [3, 3]], [[2, 5], [3, 4]] \\ &], \\ &[[2, 6], [3, 3]], [[2, 6], [3, 5]], [[3, 1], [4, 1]] \\ &], \\ &[[3, 2], [4, 1]], [[3, 3], [4, 1]], [[3, 4], [4, 1]] \\ &], \\ &[[3, 5], [4, 1]]] \end{aligned} $	
11	(1,7,6,1)	$ \begin{aligned} &[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]] \\ &], \\ &[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]] \\ &], \\ &[[1, 1], [2, 7]], [[2, 1], [3, 1]], [[2, 1], [3, 2]] \\ &], \\ &[[2, 1], [3, 3]], [[2, 2], [3, 1]], [[2, 2], [3, 4]] \\ &], \\ &[[2, 2], [3, 5]], [[2, 3], [3, 1]], [[2, 3], [3, 6]] \\ &], \\ &[[2, 4], [3, 2]], [[2, 4], [3, 4]], [[2, 4], [3, 6]] \\ &], \\ &[[2, 5], [3, 2]], [[2, 5], [3, 5]], [[2, 6], [3, 3]] \\ &], \\ &[[2, 6], [3, 4]], [[2, 7], [3, 3]], [[2, 7], [3, 5]] \\ &], \\ &[[2, 7], [3, 6]], [[3, 1], [4, 1]], [[3, 2], [4, 1]] \\ &], \\ &[[3, 3], [4, 1]], [[3, 4], [4, 1]], [[3, 5], [4, 1]] \\ &], \\ &[[3, 6], [4, 1]]] \end{aligned} $	$e_i^2 = e_i, e_i e_j = e_j e_i = 0 \text{ при } i \neq j$
12	(1,7,7,1)	$[[[1, 1], [2, 1]], [[1, 1]$	$r_i r_j = r_j r_i = 0, e^2 = e, e r_i = 0,$

		$ \begin{aligned} &], [2, 2]], [[1, 1], [2, 3] \\ &], \\ &[[1, 1], [2, 4]], [[1, 1] \\ &], [2, 5]], [[1, 1], [2, 6] \\ &], \\ &[[1, 1], [2, 7]], [[2, 1] \\ &], [3, 1]], [[2, 1], [3, 2] \\ &], \\ &[[2, 1], [3, 3]], [[2, 2] \\ &], [3, 1]], [[2, 2], [3, 4] \\ &], \\ &[[2, 2], [3, 5]], [[2, 3] \\ &], [3, 1]], [[2, 3], [3, 6] \\ &], \\ &[[2, 3], [3, 7]], [[2, 4] \\ &], [3, 2]], [[2, 4], [3, 4] \\ &], \\ &[[2, 4], [3, 6]], [[2, 5] \\ &], [3, 2]], [[2, 5], [3, 5] \\ &], \\ &[[2, 5], [3, 7]], [[2, 6] \\ &], [3, 3]], [[2, 6], [3, 4] \\ &], \\ &[[2, 6], [3, 7]], [[2, 7] \\ &], [3, 3]], [[2, 7], [3, 5] \\ &], \\ &[[2, 7], [3, 6]], [[3, 1] \\ &], [4, 1]], [[3, 2], [4, 1] \\ &], \\ &[[3, 3], [4, 1]], [[3, 4] \\ &], [4, 1]], [[3, 5], [4, 1] \\ &], \\ &[[3, 6], [4, 1]], [[3, 7] \\ &], [4, 1]]] \end{aligned} $	$r_i e = r_i$
13	(1,7,7,1)	$ \begin{aligned} &[[[1, 1], [2, 1]], [[1, 1] \\ &], [2, 2]], [[1, 1], [2, 3] \\ &], \\ &[[1, 1], [2, 4]], [[1, 1] \\ &], [2, 5]], [[1, 1], [2, 6] \\ &], \\ &[[1, 1], [2, 7]], [[2, 1] \\ &], [3, 1]], [[2, 1], [3, 2] \\ &], \end{aligned} $	$ \begin{aligned} &r_i r_j = r_j r_i = 0, e^2 = e, r_i e = 0, \\ &e r_i = r_i \end{aligned} $

		$ \begin{aligned} & [[2, 1], [3, 3]], [[2, 2], [3, 1]], [[2, 2], [3, 4]], \\ & [[2, 2], [3, 5]], [[2, 3], [3, 1]], [[2, 3], [3, 6]], \\ & [[2, 3], [3, 7]], [[2, 4], [3, 2]], [[2, 4], [3, 4]], \\ & [[2, 4], [3, 6]], [[2, 5], [3, 2]], [[2, 5], [3, 5]], \\ & [[2, 5], [3, 7]], [[2, 6], [3, 3]], [[2, 6], [3, 4]], \\ & [[2, 6], [3, 7]], [[2, 7], [3, 3]], [[2, 7], [3, 5]], \\ & [[2, 7], [3, 6]], [[3, 1], [4, 1]], [[3, 2], [4, 1]], \\ & [[3, 3], [4, 1]], [[3, 4], [4, 1]], [[3, 5], [4, 1]], \\ & [[3, 6], [4, 1]], [[3, 7], [4, 1]] \end{aligned} $	
--	--	--	--

3.4. Построение диаграмм

Используя полученную в пунктах 3.1, 3.2 и 3.3 информацию, строится диаграмма решетки подалгебр алгебры S . Построение осуществляется в несколько этапов:

1. Изображаются подалгебры алгебры S точками (или кружочками).
2. Изображается отношение покрытия, соединяя покрываемый элемент с покрывающим отрезком.

Таким образом, в работе доказано, что все трехмерные немоногенные подалгебры делятся на семь разных типов по виду решеток. Построены диаграммы всех решеток и проверены на изоморфизм, оказалось, что внутри каждого

типа, за исключением типа $(1, 4, 4, 1)$, подалгебры имеют изоморфные решетки подалгебр. Подалгебры с типом решетки $(1, 4, 4, 1)$ делятся на два подмножества и имеют неизоморфные решетки подалгебр.

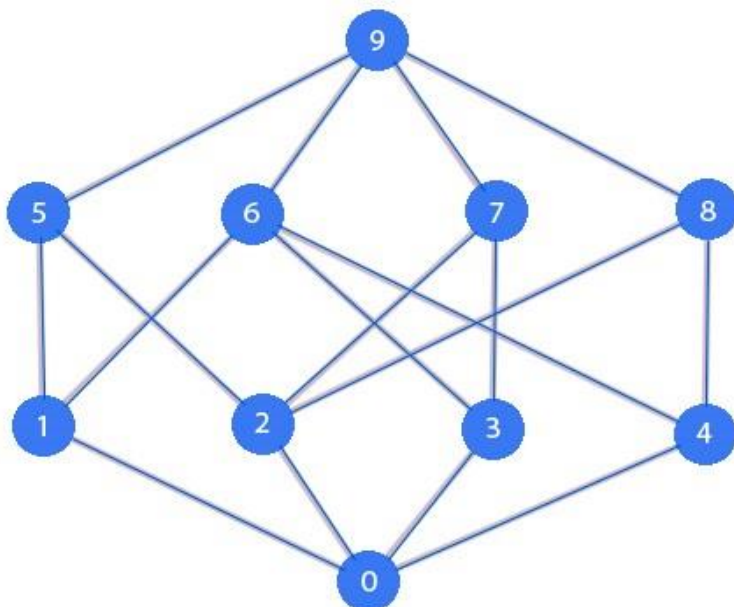


Рисунок 1. Тип $(1,4,4,1)$

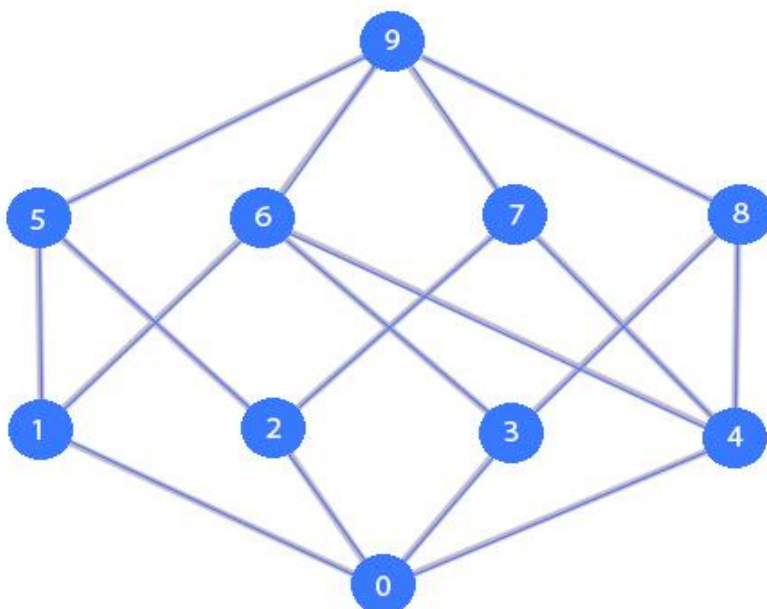


Рисунок 2. Тип $(1,4,4,1)$

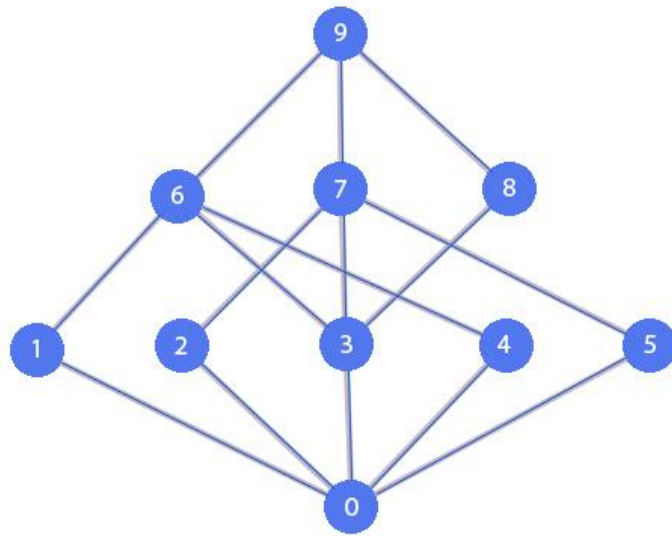


Рисунок 3. Тип (1,5,3,1)

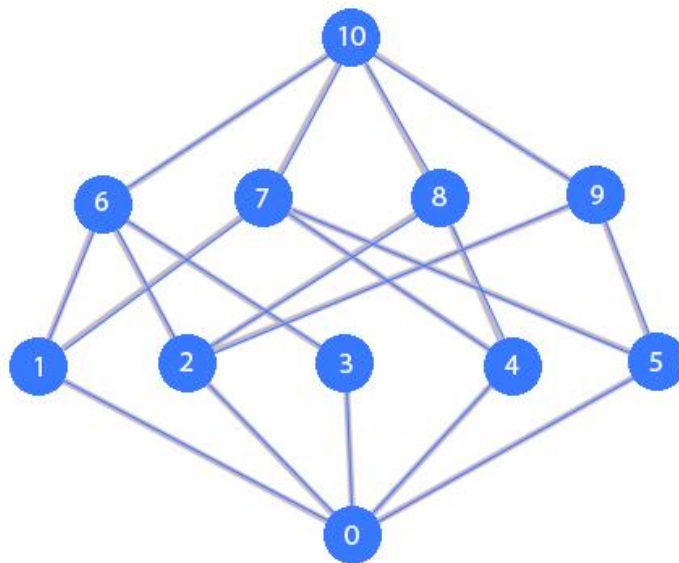


Рисунок 4. Тип (1,5,4,1)

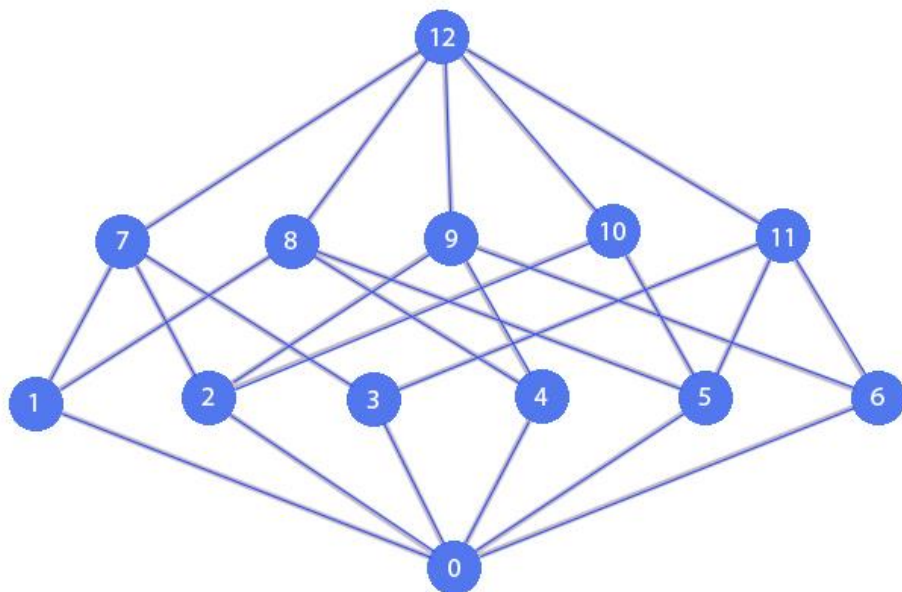


Рисунок 4. Тип (1,6,5,1)

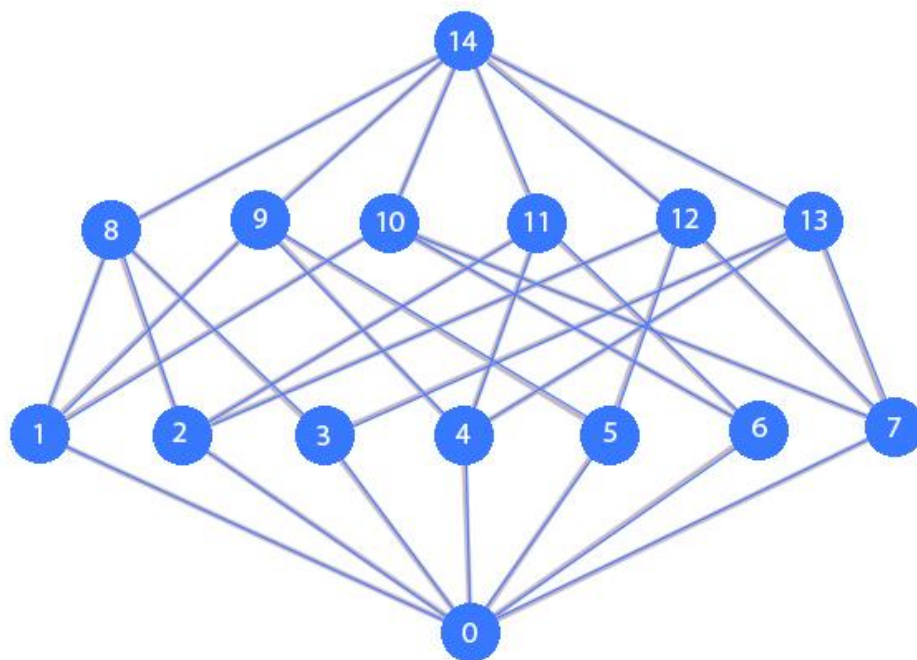


Рисунок 4. Тип (1,7,6,1)

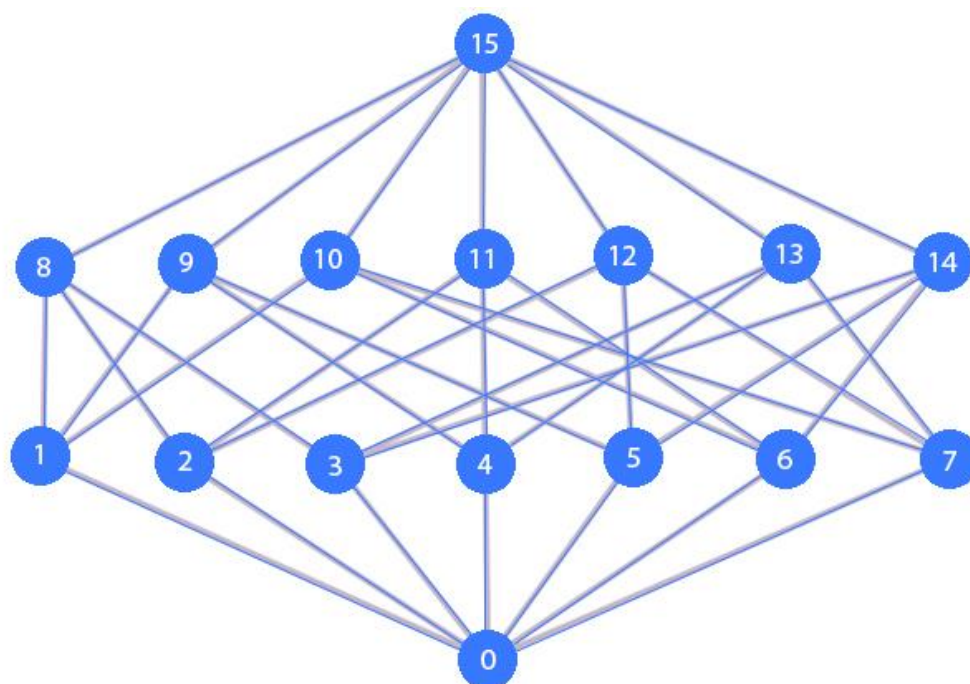


Рисунок 4. Тип (1,7,7,1)

Литература

1. Биркгоф Г., Барти Т. К. Современная прикладная алгебра; пер. с англ. Ю. И. Манина. – Изд. 2-е, стер. – М.: Лань, 2005. – 400 с.
2. Биркгоф, Г. Теория решеток; пер. с англ. В. Н. Салий под ред. Л. А. Скорнякова. – М.: Наука, 1984. – 568 с.
3. Гантмахер Ф.Р. Теория матриц. – 4 изд. – М.: Наука. Гл. ред. физ.-мат. лит. 1988.
4. Гретцер, Г. Общая теория решеток; пер. с англ. А. Д. Больбота, В. А. Горбунова, В. И. Туманова под ред. Д. М. Смирнова. – М.: Мир, 1982. – 456 с.
5. Калужнин, Л. А. Введение в общую алгебру. – М.: Наука, 1973. – 448 с.
6. Коробков С. С. Введение в теорию решеток: Учеб. пособие по спец. курсу. Урал. гос. пед. ун-т. — Екатеринбург: Б.и., 1996. – 64 с.
7. Курош А. Г. Курс высшей алгебры: Учеб. для студентов вузов по спец. "Математика", "Прикладная математика". – 13-е изд., стер. – СПб.: Лань, 2004. – 432 с.
8. Курош А. Г. Лекции по общей алгебре: учебник. – СПб.: Лань, 2005. – 560 с.
9. Коробков С.С. Вычисления в матричных алгебрах (Прикладные аспекты алгебры и информатики). (Рукопись). Екатеринбург, 2014.
10. Гришина А.А. Подалгебры матричной алгебры $M_3(GF(2))$. Дипломная работа. УрГПУ. Екатеринбург. 2003.
11. Barnes D.W. Lattice isomorphisms of associative algebras // J. Austral. Math. Soc. 1966. V. 6. № 1. P. 106 – 121.
12. Система компьютерной алгебры GAP – Exponenta. Режим доступа: www.exponenta.ru/soft/others/gap/1.asp
13. GAP Manual. Режим доступа: <http://www.gap-system.org/Doc/manuals.html>
14. Graph Online URL: <http://graphonline.ru/>
15. Учебное пособие / А.С. Бортаковский, А.В. Пантелеев. – 3-е изд., стер. – М.: НИЦ ИНФРА-М, 2015. – 592 с.

Приложение

Массив матриц алгебры $A = M_3(GF(2))$

[illegible]

60

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]